Universitat de Lleida
Escola Politècnica Superior
Enginyeria Tècnica en Informàtica de Sistemes
Treball Final de Carrera

# Internet Rural

Autor: Jordi Malla Esqué
Director: Manuel Rami Perat
Codirector: Enric Guitart Baraut

23 de setembre de 2007

# Índex

# Índex de figures

# Índex de taules

# Capítol 1

# Introducció.

Durant els últims anys s'ha produït un considerable augment de les comunicacions mòbils i, més en concret, de les comunicacions LAN (*Local Area Network*) mòbils o Wireless LAN, mitjançant les quals es pretén donar connexió a les LAN cablejades com si es tractès d'una expansió de les mateixes, amb una particularitat, la mobilitat que ens ofereixen degut al medi que utilitzen: l'aire.

Amb l'aprovació de l'estàndard 802.11, l'any 1997, les xarxes Wireless van rebre l'empenta necessària per començar la seva implantació; una implantació que, avui en dia, es troba molt estesa pel que fa a solucions tecnològiques de xarxes locals.

Degut a l'acceptació i a l'augment d'exigències de la societat s'està desenvolupant el protocol WiMAX ( *Worldwide Interoperability for Microwave Access* ), mitjançant el protocol 802.16, per a donar cobertura a grans extensions a una velocitat més elevada. En l'actualitat, s'està treballant en diferents protocols com 802.11n, entre altres, per tal d'augmentar les prestacions de les xarxes Wireless.

El principal objectiu d'aquest Projecte, és realitzar una implantació d'una xarxa Wireless d'àrea local, WLAN, en la localitat de San Esteban de Litera i donar accés a Internet.

Les motivacions d'aquest Projecte han estat principalment dues: en primer lloc, l'interès personal en realitzar un projecte d'enginyeria proper a la realitat, observar les necessitats d'un grup de gent, estudiar les diferents opcions existents, decidir la més adient i realitzar la implantació final, juntament amb els pressupostos; i, en segon lloc, la barrera tecnològica que existeix entre el mon rural i l'urbà. En l'actualitat, tant Catalunya, com la resta d'Espanya, ens

trovem en la cua Europea de la tecnologia.

El Projecte està dividit en quatre grans blocs: el primer, està dedicat a l'estudi teòric de les tecnologies existents i al marc legal que les afecta (dins d'aquest bloc, trobem el capítol 2); el segon, està dedicat a l'anàlisi del territori on es vol realitzar la implantació (en aquest bloc, està contingut el capítol 3, en el que podem trobar els estudis de terreny de població, entre altres); el tercer, fa referència al disseny i muntatge de la xarxa (en aquest, s'engloben els capítols 4 . En ell podem observar la topologia de la xarxa i els aparells necessaris per realitzar la implantació); i, el quart i últim, engloba un el pressupost de la implantació del Projecte i una visió global sobre l'actualitat de les operadores (el capítol 5 i 6 es troben englobat en aquest bloc).

Tot i que, un dels principals objectius del Projecte és fer la implantació complerta, degut a problemes burocràtics i de temps, no s'ha pogut realitzar la part més pràctica , així doncs, tots els càlculs que es realitzen són teòrics, tot i això, s'ha intentat que sigui el més fidel possible a la realitat de la Població.

# Capítol 2

# Marc tecnològic i legal.

Per tal de dur a terme el Projecte, en primer lloc, s'ha fet un estudi de les tecnologies inalàmbriques més utilitzades actualment, més concretament s'ha realitzat l'estudi sobre les tecnologies WiFi (*Wireless Fidelity*) i WiMAX. Tot seguit, es passa a detallar els aspectes legals que cal tenir en compte a l'hora d'utilitzar aquestes tecnologies en l'àmbit del Projecte.
L'estudi de les tecnologies inalàmbriques s'ha centrat en els següents punts principals:

1. Definició dels estàndards de cada tecnologia.
2. Organismes que gestionen els estàndards.
3. Funcionament de la tecnologia.
4. Topologia de la xarxa.
5. Arquitectura de la xarxa.
6. I, Seguretat.

Pel que fa al marc legal, s'enumera els passos que s'han de tenir en compte per tal d'establir-se com a operador i el per qué de la necessitat d'establir-se com a operadora, així com, les bandes de freqüència a utilitzar per les tecnologies enumerades anteriorment.

## 2.1 Tecnologies inalàmbriques.

Per tal de dur a terme les connexions inalàmbriques, s'ha centrat l'estudi en dues tecnologies Wireless: WiFi i WiMAX. El per qué d'aquestes dues tecnologies, i no d'altres, és bén senzill:

- Primer: perquè tant WiFi com WiMAX son dos estàndards aprovats per l'IEEE (*The Institute of Electrical and Electronics Engineers*), tant per a dispositius fixos, com mòbils.
- Segon: WiFi és la tecnologia inalàmbrica més utilitzada fins al moment pel que es refereix a xarxes inalàmbriques, WLAN (*Wireless Local Area Network*).
- I, tercer: WiMAX és una tecnologia en clara evolució ascendent, que ens permet complementar perfectament a WiFi, per tal d'expandir el concepte de xarxa inalàmbrica a gran escala, WMAN (*Wireless Metropolitan Area Network*).

### 2.1.1 Història

Per començar a familiaritzar-nos amb els protocols de comunicació inalàmbrics, es farà una mica d'història de les comunicacions inalàmbriques, des de la seva creació, fins a l'actualitat.

El 14 de maig de 1897, Guillermo Marconi va realitzar la primera transmissió via radio de la història, però l'existència de les ones electromagnètiques va ser predita per Heinrich Hertz, que va ser el primer en crear ones de radio en un laboratori. A Marconi se'l considera el pare de les connexions inalàmbriques, ja que, va ser el primer en enviar missatges a través de les ones de radio, això li va suposar el Premi Novel de Física el 1909.

A mitjans anys 80 als laboratoris d'IBM a Zurich, Suïssa, els enginyers que hi treballaven van desenvolupar l'idea d'una connexió entre equips, sense la necessitat d'utilitzar cables. El primer intent va ser una connexió mitjançant infrarojos, una connexió molt limitada, ja què, només permet connexions a vista sense cap obstacle entre la comunicació. Tot seguit, es va començar a implementar les comunicacions utilitzant l'espectre radioelèctric.

Després de molts prototips a diferents freqüències i diferents tecnologies, es van adonar que aquesta tecnologia podria tenir una importància rellevant en un

futur proper. Així doncs, es va decidir crear uns protocols per tal d'estandarditzar els productes i tenir una compatibilitat mundial.

Es va crear un estàndard Europeu, el HiperLan, desenvolupat per l'Institut d'Estàndards de Telecomunicacions Europeus i un al Estats Units, 802.11, desenvolupat l'any 1997 per l'IEEE, dels dos estàndards el que s'ha acabat imposant ha estat el 802.11.

Aquesta norma s'ha anat revisant any a any, introduïnt noves modificacions per tal de millorar en la seguretat, protecció, velocitat de les dades, accés al medi, etc. Avui en dia, encara hi ha estàndards en procés de desenvolupament , i, constant adaptació a les exigències de les comunicacions actuals.

Un exemple de la constant evolució de les xarxes Wireless és l'estàndard 802.16, més conegut com WiMAX, que permet la connexió inalàmbrica a distàncies superiors al Wi-Fi, i, també, incorpora el concepte de NLOS (*Non-line-of-sight*), que ve a ser, comunicació sense visió directa.

### 2.1.2 WiFi

L'estàndard WiFi, nom que s'utilitza per definir qualsevol variant de l'estàndard 802.11, fou dissenyat per substituir a les capes Física i MAC (*Medium Acces Control*) de la norma 802.3; estàndard que utilitza ethernet.

L'únic que diferencia una xarxa ethernet d'una xarxa Wireless, és l'accés al medi; la resta, és idèntica. Per tant, una xarxa Wireless és completament compatible amb tots els serveis d'una xarxa cablejada.

Hi ha quatre tipus de WiFi, basats, cadascun d'ells, en l'estàndard 802.11, que són els següents: 802.11a, 802.11b, 802.11g i 802.11n, el qual està previst que s'aprovi a l'octubre del 2008.

Els estàndards 802.11b i 802.11g gaudeixen de gran acceptació degut a la banda de freqüències que utilitzen de 2,4 Ghz, banda liberalitzada quasi universalment, amb una velocitat màxima teòrica de 11Mbps i 54 Mbps, respectivament. Aquest dos estàndards son compatibles entre ells.

Pel que fa a l'estàndard 802.11a, la seva acceptació ha estat menor, degut a la banda de freqüències utilitzada de 5GHz; una freqüència liberalitzada recentment. Per altra banda, els 5GHz, és una freqüència poc utilitzada, per tant, ens garanteix poques interferències amb altres productes. Un dels principals inconvenients d'aquest protocol, és que necessita de visió directa entre transmissor i receptor, ja què, en cas contrari, les pèrdues són majors que en l'estàndard 802.11b/g. La seva velocitat màxima teòrica és de 54Mbps.

L'estàndard 802.11a no és compatible amb l'estàndard 802.11b/g, degut a la diferència de freqüències utilitzades.

L'estàndard 802.11n, treballarà en les freqüències de 2,4 i 5 Ghz, per tant, el fa compatible amb els estàndards 802.11a, 802.11b i 802.11g. En aquest estàndard, i per tal d'augmentar la velocitat de transmissió a 248Mbps, s'introdueixen conceptes com MIMO (*Múltiple Input Múltiple Output*) i la utilització de tres antenes per dur a terme les transferències.

Per tal de realitzar aquest Projecte es compararan dos dels estàndards enumerats anteriorment, 802.11g i 802.11a i s'ha decidit discutir sobre aquests estàndards per diferents motius:

1. En el cas de l'estàndard 802.11g, primer, per la seva adaptació i implantació actual, ja què, és el numero 1 en aquest aspecte.

2. I, en el cas del 802.11a, per les possibilitats que ens dóna al treballar en la freqüència de 5Ghz, interferències, velocitat, implantació, .... .

3. S'ha descartat el protocol 802.11n, tot i ser millor que els dos anteriors, perquè es troba en fase de proves i per la seva falta d'equips homologats.

#### 2.1.2.1 Estàndard 802.11a i 802.11g

Els dos estàndards estan basats en el protocol 802.11 en l'únic que difereixen es en la freqüència emprada i en la modulació del senyal, així doncs, passarem a explicar com funciona el protocol 802.11.

Tot seguit es passa a enumerar i comentar alguns dels aspectes de la tecnologia que utilitza el protocol 802.11a/g, aspectes com: el funcionament general, la modulació, la topologia de la xarxa i la seguretat, en aquesta última part és farà una major reflexió, ja que, és un dels cavalls de batalla dels protocols Wireless.

#### 2.1.2.2 Funcionament protocol 802.11.

Una xarxa local 802.11 està basada en una arquitectura cel·lular on el sistema, denominat BSS (*Basic Service Set*), està dividit amb cel·les, i, cadascuna d'aquestes està controlada per un AP (*Acces Point*) o estació base.

Tot i que, una xarxa Wireless pot estar formada únicament per una única cel·la, habitualment es configuren per funcionar amb més d'una cel·la.

La comunicació entre punts d'accés es pot fer mitjançant ethernet, que es l'habitual, o mitjançant Wireless.

La xarxa Wireless completa, incloent les diferents cel·les i els seus punts d'accés, es poden veure en el model ISO/OSI (*International Organization for Standardization/Open Systems Interconnection*) com una xarxa 802 clàssica, i és denominada, en els estàndards, com Conjunt Estès de Serveis (ESS).

#### 2.1.2.3 Wi-Fi Alliance.

És una associació internacional sense ànim de lucre que fou fundada el 1999. Es va formar per certificar la interoperabilitat dels productes WLAN, basats en l'especificació IEEE 802.11

Qualsevol equip que obtingui el certificat de la Wi-Fi Alliance, pot interactuar amb qualsevol altre dispositiu amb el mateix logotip, tot i que, estiguin fabricats per diferents marques. Això, ens dona una certa tranquil·litat a l'hora de comprar els productes, ja què, no hem de buscar marques especifiques, si no productes que compleixin la normativa IEEE 802.11, és a dir, que tinguin el logotip de la Wi-Fi Alliance.


Figura 2.1: Logotip del certificat de la Wi-Fi Alliance.

Depenent de l'estàndard que utilitzi el producte, 802.11a, 802.11b, 802.11g , pot obtenir un certificat ò un altre, ò, fins i tot, més d'un.


Figura 2.2: Certificat 802.11a


Figura 2.3: Certificat 802.11b


Figura 2.4: Certificat 802.11a/b


Figura 2.5: Certificat 802.11b/g


Figura 2.6: Certificat 802.11a/b/g

#### 2.1.2.4 Modulació WiFi.

El protocol 802.11a, utilitza la modulació d'espectre d'extensió de seqüència directa (DSSS).

El protocol 802.11g utilitza la modulació per multiplexació de divisió en freqüències ortogonals (OFDM) .

#### 2.1.2.5 Topologia xarxa Wireless.

Pel que fa a la topologia d'una xarxa que utilitza 802.11, ens podem trobar amb dos casos, Xarxa Ad-hoc, Xarxa Infraestructura.

- **Xarxa Ad-hoc.**

  En aquest tipus de topologia els equips s'interconnecten entre si, sense la intervenció de cap punt d'accés, és a dir, es realitza una connexió, punt a punt, entre els dos equips que es volen comunicar; l'únic que s'ha de tenir en compte és què, tant emissor, com receptor, han de transmetre pel mateix canal i han de tenir el mateix identificador de xarxa configurat, ESSID.

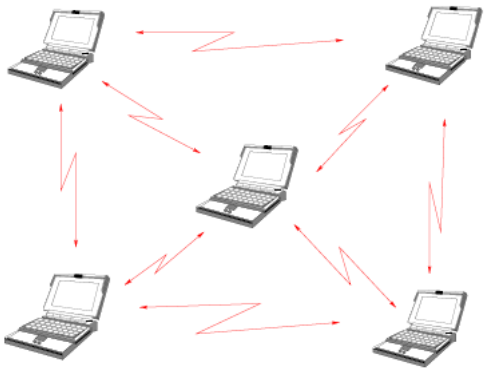

Figura 2.7: Esquema Ad-hoc

- **Xarxa Infraestructura.**

  Aquest mode utilitza els AP per interconnectar equips de la xarxa. Aquesta característica, permet encaminar els paquets, des de l'origen, fins al destí.

  La configuració del canal es produeix de manera automàtica per part de la targeta Wireless de l'equip, això, ens permet configurar el canal a l'AP més proper a l'equip, de manera automàtica. En una xarxa en mode infraestructura, els AP poden treballar en root mode, bridge mode, repeater mode i, alguns, permeten el mode WDS (*Wireless Distribution System*).

1. Root mode: L'AP, que es torba configurat amb aquest mode, és el que s'encarrega d'enllaçar la xarxa Wireless amb la LAN.
2. Bridge mode: Amb aquest mode l'AP, només es pot comunicar amb altres AP's.
3. Repeater mode: Si l'AP es torba en aquest mode, repeteix el senyal, tant per AP's, com per Clients Wireless.
4. WDS mode: Permet a un AP comunicar-se amb altres AP's, Bridge mode, i, a la vegada, comunicar-se amb Clients Wireless.

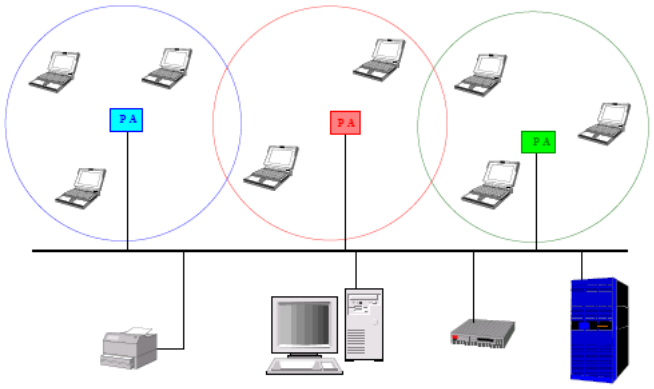

Figura 2.8: Esquema Wireless

El concepte de canal enumerat anteriorment està relacionat amb les freqüències de treball de les xarxes Wireless. En les xarxes inalàmbriques, el conjunt de freqüències del que es disposa per emetre, es divideixen en canals, i cadascun d'ells tindrà una freqüència central i un ample de banda.

Les xarxes Wireless disposen de 11 canals per tal de comunicar els AP's amb els Clients. Això ens serveix, per exemple, si en un bloc de pisos ens trobem amb diferents AP's i no volem interferències entre ells, llavors, hem de configurar els AP's en canals diferents. Quant és configura un canal s'ha de tenir pressent la següent taula:

| Identificador de canal | Freqüènica en MHz |
|---|---|
| 1 | 2412 |
| 2 | 2417 |
| 3 | 2422 |
| 4 | 2427 |
| 5 | 2432 |
| 6 | 2437 |
| 7 | 2442 |
| 8 | 2447 |
| 9 | 2452 |
| 10 | 2457 |
| 11 | 2462 |

Taula 2.1: Taula de canals i freqüències. 802.11b/g

| Identificador Canal | Freqüència MHz |
|---|---|
| 36 | 5180 |
| 40 | 5200 |
| 44 | 5220 |
| 48 | 5240 |
| 52 | 5260 |
| 56 | 5280 |
| 60 | 5300 |
| 64 | 5320 |

Taula 2.2: Taula de canals i freqüències. 802.11a

Tal i com es pot comprovar en la taula, les freqüències es troben separades per 5 MHz, tenint en compte que l'ample de banda del canal és de 22 MHz, es dedueix que, per tal d'evitar les interferències, en cas d'utilitzar més d'un canal en un lloc determinat, la separació entre canals ha de ser de 4 canals. Per exemple, en un mateix lloc es podran utilitzar el canal 1, 6 i 11.

#### 2.1.2.6 Arquitectura de les xarxes WiFi.

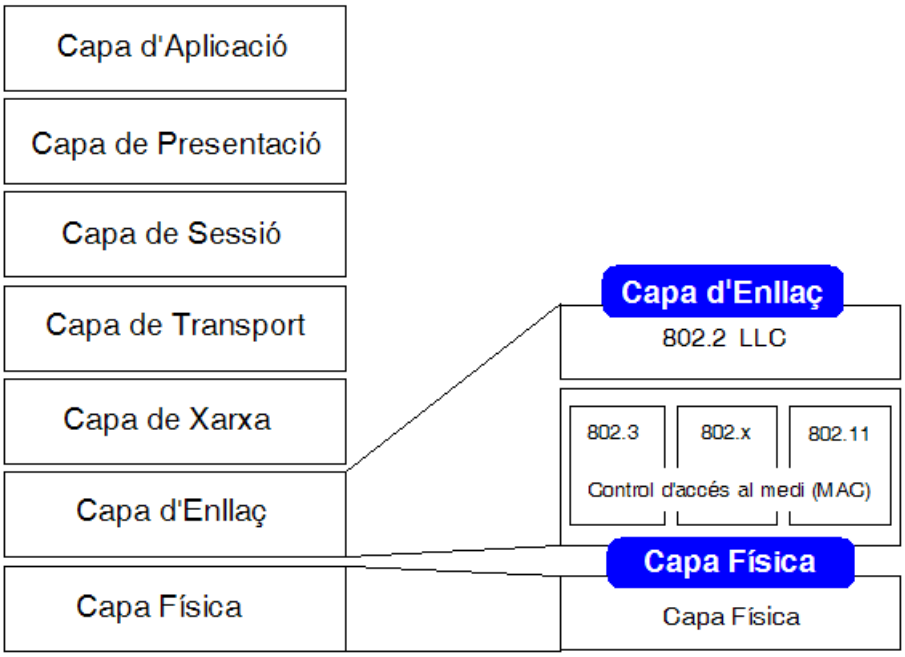


Figura 2.9: Arquitectura xarxes WiFi.

– Subcapa d'accés al medi (MAC):

L'arquitectura MAC s'encarrega de gestionar l'accés al medi.

Al nivell inferior, podem torbar la Coordinació Distribuïda (DCF) que es basa en tècniques d'accés aleatori al medi, les seves principals característiques són:

- Utilitza MACA (*Medium Access Collision Avoidance*), SMA/CA (*Carrier Sense Multiple Access with Collision Detection*) amb RTS/CTS (*RTS/CTS*)) com a protocol d'accés al medi.
- Necessita el reconeixement de ACK's (*ACKnowledged*).
- Utilitza un camp Duration/ID que conté el temps de reserva per la transmissió i ACK.

- Implementa fragmentació de dades.
- Concedeix prioritat entre trames mitjançant l'espaiat entre trames (IFS).
- Suporta Broadcast i Multicast sense ACKs.

#### 2.1.2.7 Seguretat en les xarxes WiFi.

Per tal de garantir la integritat i l'autenticitat de les dades en l'estàndard WiFi, es farà un repàs sobre els diferents protocols i/o mètodes que hi han hagut al llarg de l'existència de WiFi, com són: El filtratge de direccions MAC, Protocol WEP, WPA i WPA2, 802.1x, Servidor IAS (*Internet Authentication Service*) RADIUS (*Remote Authentication Dial In User Service*).

– **El filtratge de direccions MAC.**

El filtratge per direccions MAC, consisteix en mantenir un llistat de direccions MAC en el punt d'accés dels equips que estan autoritzats a connectar-se a la xarxa. D'aquesta manera, els equips que no figurin en aquesta llista no es podran connectar. Aquest mètode reporta uns quants desavantatges:

1. Si hi ha molts AP, ens suposaria molt treball mantenir totes les llistes i el teclejar repetidament una mateixa direcció MAC, pot donar lloc a errors ,amb la qual cosa, es denegaria el servei a usuaris autoritzats.
2. La transmissió en WiFi es fa per paquets, i, dins dels mateixos, hi viatja la direcció MAC en text pla, per tant, no és gens difícil, per a un hacker, capturar el paquet i obtenir una MAC autoritzada.
3. La direcció MAC és una característica del hardware, no de l'usuari, per tant, si la tarja es perdés, ò fos robada, el sistema de seguretat quedaria vulnerat.

– **Protocol d'encriptació WEP (*Wired Equivalent Privacy*).**

El protocol d'encriptació WEP consisteix en donar una clau privada a cada punt d'accés, la qual serà compartida pels usuaris que es vulguin connectar. Aquesta clau te una longitud de 64 o 128 bits i és donada en hexadecimal o en ASCII ( 64bits, 5 caràcters i 128bits, 13 caràcters), per definició del mateix protocol la clau sempre és fixa i no es canvia, a no ser què, ho faci l'administrador, de manera manual. Amb aquesta

clau, l'algorisme RC4 i un vector d'inicialització (IV) es realitza el xifrat. Debilitats del protocol WEP:

1. El vector d'inicialització (IV) és molt curt (24 bits) i, això, ocasiona que en xarxes amb molt tràfic es repeteixi molt sovint.
2. Hi ha targes que generen vectors molt senzills, com pot ser, començar per 0 i incrementar 1 cada vegada, cosa què, és fàcil d'encertar.
3. Les claus utilitzades són estàtiques i no és fàcil canviar-les freqüentment.
4. No te un control de seqüència de paquets, per tant, pot ser que hi hagi paquets robats i/o modificats dins la comunicació.

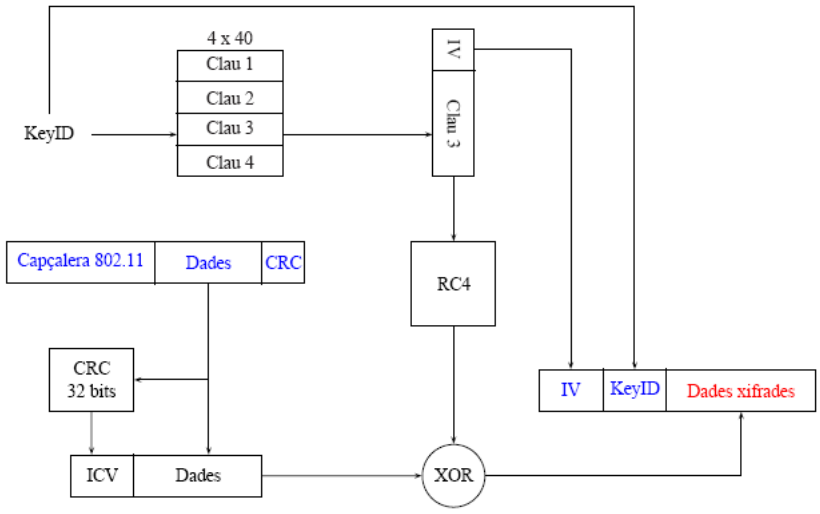


Figura 2.10: Esquema de blocs, xifratge WEP.

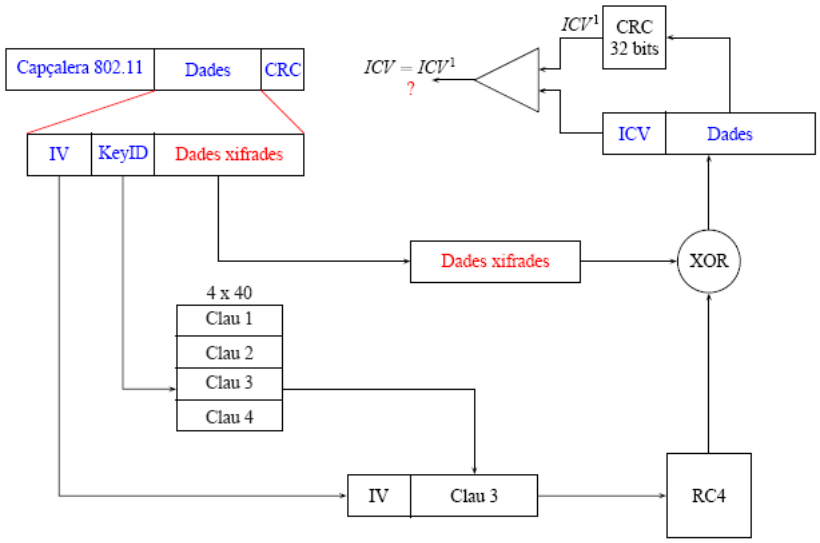


Figura 2.11: Esquema de blocs, desxifratge WEP.

– **Protocol d'encriptació WPA (*Wi-Fi Protected Access*).**

Els protocols d'encriptació WPA i WPA2 van ser la solució de la WiFi Alliance a la vulnerabilitat del protocol WEP.

El protocol WPA, es va desenvolupar per actualitzar els productes ja existents fins a la data. L'actualització consisteix en el protocol TKIP (*Temporal Key Integrity Protocol*), el qual embolcalla al protocol WEP i és conegut com WPA. WPA és la primera fase del protocol 802.11i.

Millores introduïdes pel protocol WPA:

1. S'incrementa el vector d'inicialització de 24 a 48 bits.
2. S'afegeix una funció MIC (*Message Integrity Check)* per garantir la integritat dels missatges.
3. Les claus de sessió ara són generades dinàmicament.
4. 802.1x, estàndard que proporciona un control d'accés en xarxes basades en ports. El concepte de port, en aquest cas, s'utilitza des de la part del AP, ja què, en cada port, es connectarà un equip i aquest port

romandrà bloquejat fins que l'equip no s'autentifiqui. Amb aquest fi s'utilitza el protocol EAP (*Extensible Authentication Protocol*) i un servidor AAA (*Authentication Authorization Accounting*), com pot ser RADIUS, mitjançant el servidor IAS RADIUS. També, podem aplicar polítiques de privilegis.

5. EAP, protocol que s'encarrega de dur a terme l'autenticació.
6. TKIP, s'encarrega de generar les claus per cada trama i està basat en l'algorisme de xifratge RC4.

– **Protocol d'encriptació WPA2.**

WPA i WPA2 són molt similars en molts aspectes, la diferència principal entre tots dos, és què WPA2 utilitza el tipus de xifratge CCMP-AES (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol - Advanced Encryption Standard* ) i WPA utilitza TKIP-RC4.

També, hem de tenir en compte què, WPA2 exigeix un plus de potència de comput, a causa de la utilització de l'algorisme CCMP-AES. Aquesta part és important tenir-la en compte, ja què, equips vells, amb capacitats de comput limitades, no podran implementar WPA2.

La seguretat del protocol de xifratge WPA2 es basa en l'estàndard 802.11i i utilitza el protocol CCMP, com a mecanisme de xifrat, que utilitza com a base el famós algoritme de xifratge avançat AES de 128 bits.

Un altre dels aspectes a destacar, és la compatibilitat amb el servei de VoiP, ja què, evita el retràs de la senyal i els talls de conversa en moviment.

– **802.1x/Autentificació.**

Les modificacions que inclou el protocol 802.1x són les següents:

1. Es necessita l'autentificació dels usuaris, abans de connectar-se a la xarxa WiFi; en cap cas, s'autentifica l'equip com passava en el filtratge MAC.
2. L'autentificació es realitza mitjançant el protocol EAP.
3. L'autentificació es realitza mitjançant un servidor IAS RADIUS, això vol dir que cap AP pot autoritzar l'accés a la xarxa.

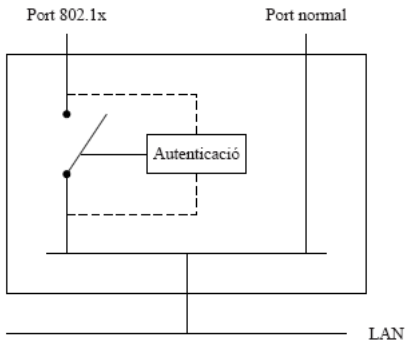


Figura 2.12: Esquema autentificació 802.1x.

– **Servidor IAS RADIUS.**

El servidor RADIUS el podem trobar habitualment com un software que complementa al O.S. (*Operating System*) ò mitjançant un appliance, hardware dedicat, ò, fins i tot, en el mateix AP.

Les principals funcions del servidor RADIUS són:

1. Rebre les peticions de connexions WiFi dels usuaris.
2. Autentificar als usuaris WiFi i després donar-los accés a la xarxa.
3. El servidor RADIUS pot generar claus dinàmiques.
4. A diferència de les VPN, protegeix la capa 2, ja què, xifra el canal abans d'assignar una IP. Per contra, VPN necessita una IP per xifrar el canal.

### 2.1.3 WiMAX

WiMAX és un estàndard de transmissió inalàmbrica dissenyat per a l'àrea metropolitana o MAN, proporcionant accessos concurrents a 50 km de radi i amb velocitats de 100Mbps, utilitzant la tecnologia portàtil LDMS (*LANDesk Management Suite*) i no necessita visió directa, entre l'estació base (BS) i l'estació subscriptora (SS).

Integra la família d'estàndards 802.16 i l'estàndard HyperMan de l'organisme d'estandardització europeu ETSI.
L'estàndard 802.16 ha donat lloc a diferents modificacions del mateix, tals com: 802.16, 802.16a, 802.16-2004 i 802.16e.
Per tal de realitzar el Projecte, es tindrà en compte l'estàndard 802.16-2004, ja què, es vol comparar aquest estàndard i el 802.11a, per tal de decidir quin és millor en aquest cas, per a una implementació punt a punt.
El funcionament del protocol és similar al del 802.11, on una estació base amb una antena controla l'accés inalàmbric de les estacions subscriptores a la xarxa. En l'únic que és diferencien, és en la velocitat de transmissió i en la cobertura.

#### 2.1.3.1 Estàndards WiMAX.

- **802.16**

  WiMAX es va iniciar amb l'estàndard 802.16 creat l'any 2003, amb les especificacions següents:

  1. L'espectre de freqüències utilitzat són 10-66Ghz
  2. Necessita de torres LOS (*Line Of Sight*), per tal de què la connexió sigui efectiva. LOS, l'únic que ens ve a dir, és que, entre les dues estacions, no hi pot haver obstacles, han de tenir una visió directa entre ells per tal de dur a terme la comunicació.
  3. Les taxes de transferència per aquesta especificació són de 32 a 132 Mbps
  4. Utilitza els següents sistemes de modulació, QPSK (*Quadrature Phase-Shift Keying*), 16QAM (*Quadrature Amplitude Modulation*) i 64QAM.
  5. I, el radi de cobertura és de 2 a 5 km.

- **802.16a**

  El següent estàndard que va implementar l'IEEE va ser 802.16a, al març del 2003, amb les següents especificacions:

  1. Utilitza les freqüències 2-11Ghz
  2. No necessita de torres amb enllaços de tipus LOS. En aquest cas, parlarem d'enllaços de tipus NLOS, i el desplegament es farà mitjançant BS, formades per antenes emissores/receptores amb capacitat de donar servei a 200 SS, que puguin donar servei a edificis complets.

3. Les taxes de transferència són de 100Mbps.
4. Utilitza la modulació OFDM amb 256 subportadores.
5. Incorpora els serveis, SLA (*Service Level Agreement*) i QoS (*Quality Of Service*).
6. SLA significa: Acord de nivell de servei, i, permet controlar si el nivell del servei ofert, compleix amb el nivell acordat entre client i proveïdor.
7. QoS significa qualitat de servei i s'utilitza per donar preferència a un determinat transit, com la VoIP (*Voice over Internet Protocol*) o el vídeo, entre altres. El que aconseguim amb això és, prioritzar determinats serveis que requereixen interacció i resposta a temps real, sobre altres que no ho requereixen.
8. I, el radi de cobertura és de 75km.

– **802.16-2004**

L'estàndard 802.16-2004 va ser aprovat al 2004 i reemplaça al protocol 802.16, 802.16a i 802.16d.

– **802.16e**

L'estàndard 802.16e va ser aprovat al 2005 i les variacions que introdueix són:

1. Incorpora el concepte de mobilitat al protocol 802.16-2004.
2. La modulació OFDMA (*Accés Múltiple per Divisió Ortogonal de Freqüència*)
3. La freqüència en que opera, 5-6Ghz.
4. Una velocitat de transmissió de 15 Mbps
5. I, un radi d'acció de 2 a 5 km.

#### 2.1.3.2 WiMAX Forum.

WiMAX Forum és un consorci d'empreses (inicialment 67; actualment, més de 100) format el 2003. El seu objectiu és proposar i promoure la interoperabilitat entre productes de BWA, complint amb els estàndards IEEE 802.16 i ETSI HiperMan, i d'aquesta manera accelerar el desplegament global d'aquesta tecnologia.

Per realitzar aquesta tasca, el WiMAX Forum ha creat el certificat WiMAX, que han de complir tots els productes compatibles amb l'estàndard 802.16.

El WiMAX Forum, és el que s'encarrega de certificar tots els productes amb el certificat WiMAX, així doncs, podem garantir què tots els productes que tinguin la certificació WiMAX seran compatibles entre ells, independentment de quin sigui el fabricant.


Figura 2.13: Certificat WiMAX

#### 2.1.3.3 Utilització de la tecnologia WiMAX.

Tot i què, no es pot definir la seva utilització, avui en dia, degut a la seva baixa implantació, el que sí podem fer és determinar quin serà el seu possible ús, tenint en compte les seves característiques.

1. **Accés de banda ampla residencial (bucle d'abonat):** Pot competir amb les línies ADSL (*Asymmetric Digital Subscriber Line*), donant accés a Internet, VoIP i serveis multimèdia com videoconferencies, vídeo sota demanda o televisió.

2. **Serveis de telecomunicacions per a PYMES:** Accés de banda ampla dedicat en llocs on no és possible arribar-hi mitjançant cablejat.

3. **Xarxes backhaul per a hotspots WLAN:** Interconnexió de banda ampla entre xarxes WLAN, donant lloc a grans xarxes de telecomunicacions inalàmbriques a una major distància.

#### 2.1.3.4 Topologia de les xarxes WiMAX.

L'estàndard 802.16-2004 defineix les següents arquitectures compatibles amb la tecnologia WiMAX.

– **Topologia PTP:** La topologia punt a punt es considera una variant de la topologia punt a multi punt, i consisteix en un receptor i un emissor.

Aquesta topologia es sol utilitzar en enllaços dedicats de llarga distància, com podria ser la connexió entre dues illes o entre dues localitats, entre altres.

- **Topologia PMP:** En la topologia punt a multi punt es defineixen els conceptes de BS, Estació Base i SS, Estació Subscriptora. La BS s'encarrega de connectar la xarxa inalàmbrica amb la xarxa cablejada (Core Network) i les SS són les estacions que utilitzen els equips clients de la xarxa inalàmbrica per connectar-se a la BS.

- **Topologia Mesh:** Com alternativa a la topologia PMP, tenim la topologia Mesh, en la qual, tenim l'opció que un SS, per arribar a connectar-se amb la BS, es connecti amb varies SS intermitjes. En aquest cas, es denomina xarxa multi-salt, amb la qual, podrem estendre el concepte de xarxa inalàmbrica, reduïnt costos, ja què, el cost d'una SS és molt inferior al d'una BS.

#### 2.1.3.5 Arquitectura del protocol 802.16

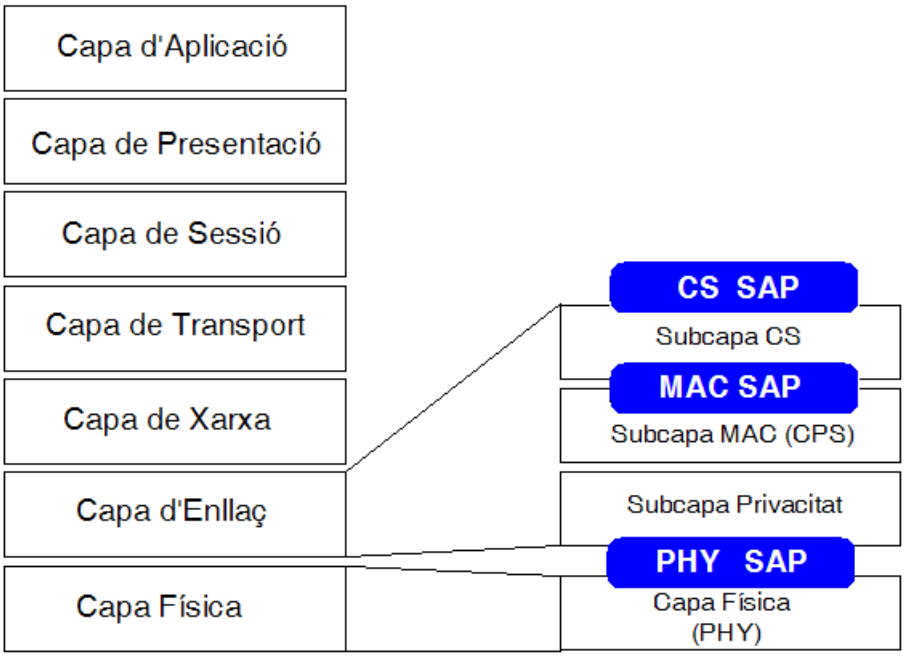


Figura 2.14: Arquitectura protocol 802.16

– Subcapa CS ( *Convergente Sublayer* ):

  Els sistemes 802.16 han de suportar xarxes ATM i xarxes de paquets (IP). La capa de convergència pot interactivar, amb aquests dos sistemes, mitjançant el Services Accés Point (SAP) i, també, s'encarrega d'interactuar amb la capa superior de la pila de protocols.

– Subcapa MAC CPS (*Common Part Sublayer*):

  Conté totes les funcions necessàries per realitzar el control d'accés al medi i l'intercanvi de dades.

– Subcapa Privacitat:

  Aquesta capa s'encarrega d'implementar els elements requerits per la privacitat, a causa de la capa física. Alguns exemples són: l'intercanvi de

claus i els processos de xifratge i desxifratge. Està interconnectada a la capa física mitjançant el Service Accés Point (PHY SAP).

– Capa Física:

Especifica els diferents modes d'operar en el medi: WirelessMAN SC, WirelessMAN Sca, WirelessMAN OFDM i WirelessMAN OFDMA.

#### 2.1.3.6 Característiques de la Capa Física.

– WirelessMAN SC:

Es tracta de la versió single carrier realitzada per a línia de visió directa (LOS) en la banda de freqüències 11 - 66 Ghz, i les opcions que suporta són: AAS (*Adaptive Antennas System*), ARQ (*Automatic Retransmision Request*), STC(*Space Time Coding*)

– WirelessMAN Sca:

Versió single carrier per a freqüències $<$ 11Ghz. Compren un conjunt de funcionalitats per suportar operacions en línia, sense visió directa (NLOS). Les opcions que suporta són: AAS, ARQ, Mesh, STC.

– WirelessMAN OFDM:

Projectada per a operacions de línia sense visió directa (NLOS) i freqüències $<$ 11 Ghz, i, utilitza com a base la modulació ortogonal. Les opcions suportades són: AAS, ARQ, Mesh, STC.

– WirelessMAN OFDMA:

Suporta operacions en NLOS a freqüències $<$ 11 Ghz. Es basa en el sistema de múltiple accés OFDMA, que es tracta d'una extensió de la tècnica OFDM per a la utilització de múltiples usuaris en un mateix canal. Suporta les mateixes opcions que Wireless OFDMA.

– WirelessHUMAN:

Comprén operacions específiques per a operar en bandes sense llicència 5 - 6 Ghz, utilitzant canals de 10 i 20 Mhz amb separacions de 5Mhz. Les opcions que suporta són AAS, ARQ, Mesh, STC.

#### 2.1.3.7 Característiques de la Subcapa MAC.

El protocol MAC de l'estàndard 802.16 està orientat a connexió; i, aquesta connexió està orientada a obtenir un cert nivell de QoS. Les connexions són bidireccionals i s'identifiquen mitjançant un identificador de 16 bits (CID).
Entre les funcions més específiques que desenvolupa la subcapa MAC, podem trobar les següents:

- Control de QoS.
- Suport per a les diferents capes físiques definides en 802.16
- Seguretat.
- Sincronisme.
- Capa de convergència per a IP i ATM (*Advanced Traffic Management*).
- Suport per a sistemes amb antenes adaptives.
- Suport a les topologies Mesh i PMP

#### 2.1.3.8 Models de propagació.

El canal de comunicació sense fils es pot definir com LOS o NLOS.
En un sistema LOS tenim que el Tx (*Transmissor*) i el Rx (*Receptor*) han d'estar en visió directa, ja què, la senyal no pot ser objecte de cap difracció. Per tal d'evitar-ho, el sistema LOS necessita que la primera zona, coneguda com Fresnel, sigui lliure d'obstacles.
En un sistema NLOS, la senyal viatja del Tx al Rx, per mitjà de reflexions i difraccions. Les senyals que arriben al Rx es composen de la senyal directa i múltiples senyals reflexades.
Alguns dels avantatges del sistema NLOS, respecte al sistema LOS són:

1. La tecnologia NLOS redueix els costos d'instal·lació, permetent una fàcil localització de l'equip client.
2. La tecnologia NLOS i les característiques del WiMAX ens permet utilitzar clients indor, tenint en compte les consideracions de potència per les pèrdues de senyal en la penetració d'edificis.

3. La tecnologia WiMAX utilitza diferents tècniques, ò tecnologies, per tal de reduïr els efectes dels enllaços NLOS (multi-camí, difracció, canvis de polarització, ...).

4. Tecnologies OFDM, Subcanalització, Antenes adaptives, Diversitat en recepció i transmissió, Tècniques de correcció d'errors (ARQ, ...), Sistemes de control de potència, Modulació o codificació adaptiva.

#### 2.1.3.9 Seguretat en les xarxes WiMAX.

La seguretat en les xarxes WiMAX ve implementada en la subcapa privacitat; subcapa què, alhora, forma part de la capa MAC.
S'encarrega de la encriptació dels fluxos de dades, entre l'estació base i les estacions client. D'aquesta manera, es garanteix la integritat de les dades i es protegeixen les comunicacions contra intrussos.
L'autentificació dels clients es realitza mitjançant un protocols de claus client / servidor. L'estació base és l'encarregada de distribuïr el material d'encriptació, protegit amb claus. Per incrementar la robustesa del protocol, s'incorpora l'autentificació dels clients mitjançant certificats digitals.
A continuació, s'explicaran els principals conceptes dels mecanismes de seguretat que ofereix WiMAX.

- Associació de Seguretat (SA).

  Una associació de seguretat és un conjunt de informació de seguretat, que comparteixen una estació base i una, o més d'una, estació client. D'aquesta manera, es pretén establir connexions segures.

  Les SA s'identifiquen amb identificadors SAID. Hi ha tres tipus de SA:

  - Primària: s'estableix una connexió de seguretat, entre una estació client i una estació base.
  - Estàtiques: les proporciona la estació base.
  - Dinàmiques: les estableix, dinàmicament, la estació base.

  La estació base és l'encarregada de mantenir la informació de seguretat, i què cada estació client només tingui accés a la SA que està autoritzat. La informació d'encriptació ( clau DES (*Data Encryption Standard*), vector d'inicialització), té un temps d'expiració, abans del qual, la estació client a de sol·licitar la nova informació, si no, haurà de reiniciar l'accés a la xarxa.

- Protocol d'autentificació.

  El procés d'autentificació d'una estació client amb l'estació base, es basa en l'intercanvi de certificats digitals, claus de reconeixement, etc... i, també, en l'intercanvi dels protocols que accepten, tant el client com l'estació base.

  Les estacions client utilitzen el Privacy Key Management (PKM) per obtenir l'autentificació de l'estació base.

  El protocol PKM utilitza EAP, certificats digitals X.509, algoritme d'encriptació RSA (Rivest Shamir Adleman) i, per intercanviar les claus, algoritmes simètrics com AES.

  El funcionament bàsic del protocol PKM és de l'estructura client-servidor. La estació client sol·licita l'accés, enviant el seu certificat digital que serà únic. La estació base revisa si el certificat digital és correcte i associa l'estació base a la xarxa. Aquest sistema, sumat amb els certificats digitals, protegeix la xarxa de possibles suplantacions d'identitat.

- Xifratge de les dades.

  La encriptació únicament s'utilitza en les trames PDU (*protocol data unit*). La capçalera genèrica MAC, els missatges MAC de gestió i el CRC (*Cyclic Redundancy Check*) s'envien en text pla, per tal de facilitar-ne la gestió.

  La encriptació de les dades es fa mitjançant dos algoritmes d'encriptació DES i AES.

Per dur a terme el Projecte s'ha de tenir molt en compte els aspectes legals, ja què, el cas que ens ocupa explota una xarxa pública de comunicacions, utilitzant l'espai radioelèctric com a medi físic. Per tant, i atenent-nos a la legislació vigent, s'ha de tenir en compte dos aspectes legals: la prestació de serveis a tercers i l'espai radioelèctric emprat.

## 2.2 Legislació vigent.

### 2.2.1 Prestació de serveis a tercers.

La Llei General de Telecomunicacions, en el seu article 6.2, i el Real Decret 424/2005, de 15 d'abril, en el seu article 5, determinen que els interessats en l'explotació d'una determinada xarxa, o en la prestació d'un determinat servei de

comunicacions electròniques, hauran de, amb anterioritat a l'inici de l'activitat, notificar-ho a la comissió del Mercat de les Telecomunicacions (CMT). Una vegada realitzada la notificació, l'interessat adquirirà la condició d'operador i podrà començar la prestació del servei o l'explotació de la xarxa.
En el mateix article 6.2 de la Llei General de Telecomunicacions, també podem trobar la documentació necessària per realitzar la notificació a la CMT. També, indica que cada 3 anys s'haurà de notificar la intenció de continuar prestant els serveis.
Per altra banda, l'article 7 de la Llei General de Telecomunicacions va crear, independentment de la CMT, el Registre d'Operadors. En ell s'han d'inscriure les dades relatives a les persones físiques o jurídiques que hagin notificat la seva intenció d'explotar xarxes o prestar serveis de comunicació electrònica, les condicions per desenvolupar l'activitat i les seves modificacions; modificacions que s'hauran de notificar, com a molt, un mes després d'haver-se produït.

No estan subjectes a l'obligació de la notificació, articles 5.4 del RD, les explotacions de xarxes, prestació de serveis en règim d'auto-prestació i els serveis prestats en una comunitat de propietaris a un immoble, o una propietat privada, sense tenir connexió amb cap xarxa de l'exterior.

1. Espai radioelèctric, potència màxima d'emissió.

   L'espai radioelèctric és un espai de domini públic, regit per el CNAF (*Quadre Nacional d'Atribució de Freqüències*), el qual s'encarrega de gestionar i adjudicar les bandes de freqüència, per tal d'assignar-les a cada servei. Tot seguit, es passa a descriure qué és l'espai radioelèctric i quines bandes de freqüència ens ocupen.

2. Definició de l'Espai radioelèctric.

   L'espai radioelèctric és de domini públic, com per exemple, les carreteres, és a dir, és d'ús comú. Ara bé, aquest espai que està gestionat per l'Admón (*Administració electrònica*) es divideix en espai d'ús comú, però també, en espai d'ús privatiu i en espai d'ús especial.

   (a) Espai d'ús comú: No es necessita cap títol habilitat per a la seva ocupació.

   (b) Espai d'ús privatiu: S'utilitza per prestar serveis de telecomunicacions. Per a la seva utilització es necessita una concessió previ pagament (Concessió administrativa per a ús de domini públic, que

consisteix en un règim d'autorització per a la utilització d'un bé que és propietat de l'Estat).

(c) Espai d'ús especial: El seu ús està reservat a l'Administració.

#### 2.2.1.1 Taxes.

Tot operador està obligat a retribuïr a l'Estat amb una taxa què, en cap cas, supera el 1,25 per mil, dels ingressos bruts obtinguts per la prestació dels serveis i l'explotació de la xarxa.

### 2.2.2 Bandes de freqüència.

El CNAF regula la utilització del domini públic radioelèctric, amb relació amb les freqüències i potències que han d'utilitzar els equips radioelèctrics que s'utilitzen per a tal efecte. En quant a les xarxes WiFi, aquestes estan regulades a la UN-51, UN-85, UN-128 i UN-107.
Els equips WiFi i/o WiMAX poden operar en les bandes de freqüència següents: ( 2,4Ghz, 3,5Ghz i 5Ghz )

- **La Banda 2400 a 2483,5 Mhz:**
- Aquesta banda es podrà utilitzar per accés inalàmbric a xarxes de comunicació electròniques, així com, per a xares d'àrea local, per a la interconnexió sense fils entre ordinadors i/o terminals. I, dispositius perifèrics per a aplicacions, preferentment, en l'interior de recintes.
- Les condicions tècniques d'ús han de ser conforme a la Decisió ERC(DEC/(01)07 i la Recomanació CEPT ERC/REC 70-03, Annex 3. La potència isotròpica radiada equivalent total, serà inferior a 100 mW (p.i.r.e.).
- **La Banda 3,5 Ghz:**

  La banda de 3400 a 3600 Mhz està destinada per a l'establiment de sistemes d'accés radioelèctrics mitjançant enllaços punt a multi punt en tot el territori nacional.
- La Banda (UNII) 5GHz està formada per tres sub-bandes, UNII1(5,15GHz - 5,25GHz), UNII2 (5,25GHz - 5,35GHz) i UNII3 (5,725 - 5,875).
- **La Banda 5150 - 5350 Mhz:**

En aquesta banda es defineix l'ús del servei mòbil en sistemes d'accés inalàmbric, incloent comunicacions electròniques i xarxes d'àrea local. Es restringeix per a la seva utilització, únicament, a l'interior de recintes i les característiques tècniques s'han d'ajustar a les indicades en la CEPT EC/DEC/(04)08.
En aquesta banda la potència isotròpica màxima radiada serà de 200mw (p.i.r.e). En la banda 5250 - 5350 Mhz la potència isotròpica de sortida serà de 100mw (p.i.r.e).

- **La Banda 5470 - 5725 Mhz:**

  Aquesta banda pot ser utilitzada per a sistemes d'accés inalàmbric a xarxes de comunicacions electròniques, així com, per a xarxes d'àrea local en l'interior o exterior de recintes.

  Les característiques tècniques s'han d'ajustar a les indicades en la CEPT ECC/DEC/(04)08.

  La potència isotròpica radiada màxima (p.i.r.e) per un transmissor ha de ser de 500 mW (p.i.r.e).

- **La Banda 5725 - 5875 Mhz:**

  Dispositius de curt abast (SRD) a la banda de 5GHz. S'autoritza els dispositius genèrics de baixa potència.

  La potència isotròpica radiada equivalent màxima es limita a 25 mW (p.i.r.e) conforme a la Decisió de la CEPT ERC/DEC/(01)06 i d'acord a les característiques tècniques indicades a l'annex 1 de la Recomanació ERC (REC 70-03 de la CEPT(*Conférence Européenne des administrations des Postes et des Télécommunications*) ).

  La norma tècnica aplicable a aquests dispositius és la EN 300 440.
  Totes les indicacions esmentades anteriorment es consideren d'ús comú. Per contra, si es vol fer qualsevol altra utilització de les bandes no esmentat en el CNAF , s'ha de demanar una concessió previ pagament a l'Estat, que seria l'equivalent a una de les antigues llicències i/o autoritzacions per a actuar en la banda requerida.

### 2.2.3 LSSI (*Ley de Servicios de la Sociedad de Información*).

En el punt 2.1 es fa referència a la prestació de serveis a tercers, cosa què implica que la persona o entitat que apliqui el Projecte, s'haurà d'establir com a operadora de telecomunicacions.

Tenint en compte aquest aspecte, un dels punts que fa referència als ISP (*Internet Service Provider*), de la llei del comerç electrònic LSSI, és el deure de la retenció de dades per part dels ISP o PSSI ( *Prestador de Serveis de la Societat de la Informació*).

La llei estableix què, l'ISP ha de conservar, durant un període d'un any, les dades següents:

- La informació necessària per a la localització d'equips informàtics que hagin estat utilitzats en la transmissió de dades, s'ha de limitar la imprescindible per a identificar l'equip i el moment de la prestació del servei.
- Aquesta informació és conservarà per a utilitzar-la en investigacions criminals, per a la seguretat pública i la defensa nacional, no podent-se utilitzar per a altres finalitats.
- La conservació de les dades queda subjecta a la observació de la normativa sobre la protecció de dades de caràcter personal.

Segons la mateixa llei aquest punt està contemplat, tot i què, encara està pendent de reglamentació, per tant, és un apartat que hem de tenir en compte per a un futur proper.

## 2.3 Llei Orgànica 15/99 de Protecció de Dades (LOPD).

Degut a l'emmagatzematge d'informació personal, s'ha de tenir present, la LOPD, la qual es passa a enumerar en els següents punts:

1. Identificar els fitxers de l'empresa i escollir el nivell de seguretat.
2. Qualsevol persona o entitat que procedeixi a la creació de fitxers de dades personals ho ha de notificar, previament, a l'Agència de Protecció de Dades.

3. Legitimar les dades de caràcter personal.

4. Crear un document de seguretat.

5. Implantar una política de seguretat.

6. Mantenir actualitzat el document de seguretat.

## 2.4 Conclusió.

Per tal de dur a terme el Projecte, s'ha decidit comparar les tecnologies Wireless i WiMAX en les bandes de freqüència 2,5 i 5Ghz, ja què, les dues són d'ús comú i no requereixen cap llicència.

En aquest apartat, també, s'ha tingut en compte el sistema legal actual, tant pel que fa a freqüències com a potències d'emissió i la necessitat d'establir-se com a operadora. Així doncs, en termes legals, el que s'haurà de tenir en compte és:

1. L'establiment com a operadora de l'interessat, complimentant la part de documentació requerida que podem trobar en l'article 6.2 de la Llei General de Telecomunicacions.

2. Segons la banda de freqüències escollides, s'ha tenir en compte la concessió previ pagament per les freqüències privatives. En aquest cas, com les freqüències escollides són d'us comú, no cal contemplar aquest cost afegit.

Un cop tenim clars els aspectes legals, podem passar a decidir la tecnologia inalàmbrica a utilitzar. Després d'una primera valoració s'ha decidit que la tecnologia a implementar serà la tecnologia Wireless, en concret l'estàndard 802.11a, el qual actúa en la freqüència de 5Ghz.

Aquesta decisió ha estat pressa en base a una millor recepció i emissió de la senyal de 5Ghz en exteriors. També s'ha escollit la tecnologia Wireless per davant de la tecnologia WiMax, degut a què, aquesta encara es troba en una primera fase experimental, on l'estàndard definitiu encara està per implementar i el cost dels equips és molt més elevat.

# Capítol 3

# Anàlisi del context de desenvolupament.

## 3.1 Estudi del terreny.

Degut a les exigències del protocol Wireless, el qual ens requereix visibilitat directa entre els punts de connexió, s'ha realitzat un estudi del terreny. Aquest estudi ha estat dut a terme pel SIG (*Sistema d'Informació Geogràfica*) a les oficines de la Universitat d'Agrònoms, de la ciutat de Lleida.

Al haver escollit el protocol Wireless és molt important que els punt de connexió tinguin visió directa.

També mitjançant aquest estudi, podrem determinar una aproximació a l'altura de les antenes: punt A, antena de San Esteban; i, punt B, antena de Binéfar.

Les connexions ha realitzar són; un enllaç entre San Esteban i Binefar, i un enllaç a Sant Esteban, amb tots els clients del poble.

### 3.1.1 Orografia del terreny.

En la imatge adjunta, es pot observar que la població de San Esteban de Litera està situada a un altura superior a la de Binéfar, per tant, tenint en compte la orografia del terreny, l'enllaç entre les dues poblacions es pot dur a terme sense problemes.

En canvi, la distribució del senyal a la població de San Esteban, requereix una major altura de l'antena degut als desnivells que presenta el terreny i les

vivendes familiars.

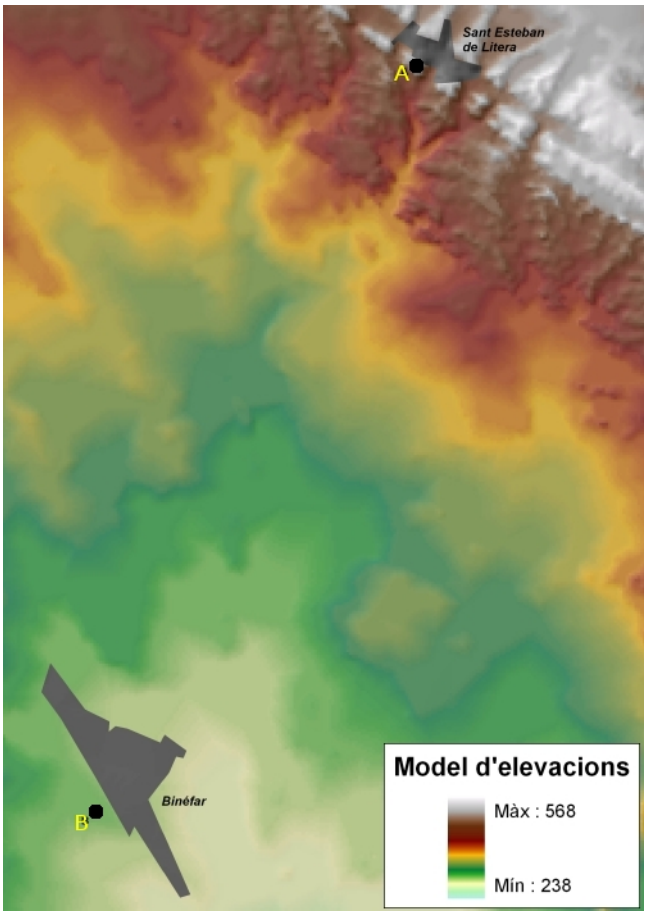


Figura 3.1: Orografia del terreny.

### 3.1.2 Visibilitat San Esteban Binéfar.

En aquest apartat, discutirem les alçades òptimes de les dues antenes que ens permetran fer l'enllaç entre San Esteban i Binéfar.

En les següents imatges cal tenir en compte dues coses: En primer lloc, l'alçada de les antenes es compta a partir del nivell de terra, ; I, en segon

lloc, la visibilitat està contemplada des del punt A a 360º. Així doncs, amb la mateixa imatge podem veure la incidència que té l'antena en els dos punts que ens interessen, l'enllaç amb Binéfar i la visibilitat dins el poble de San Esteban de Litera.

Tal i com es pot observar en les diferents imatges que es mostren a continuació, s'han fet diferents probes amb les següents alçades d'antena:

1. Antena Binéfar/San Esteban.

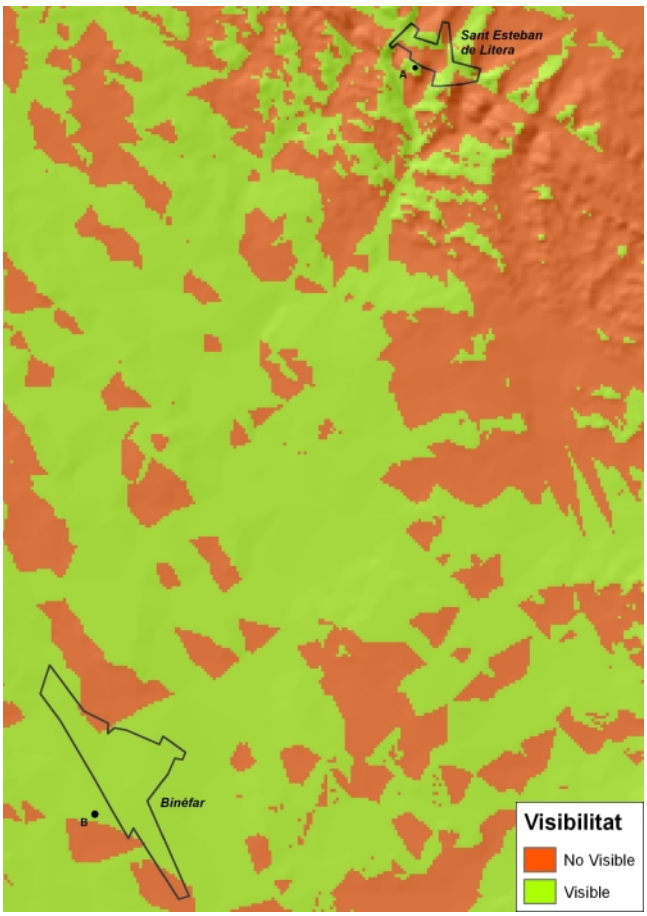


Figura 3.2: Visibilitat San Esteban, antena 10mts., Binéfar, antena 5mts.

2. Antena Binéfar/San Esteban.

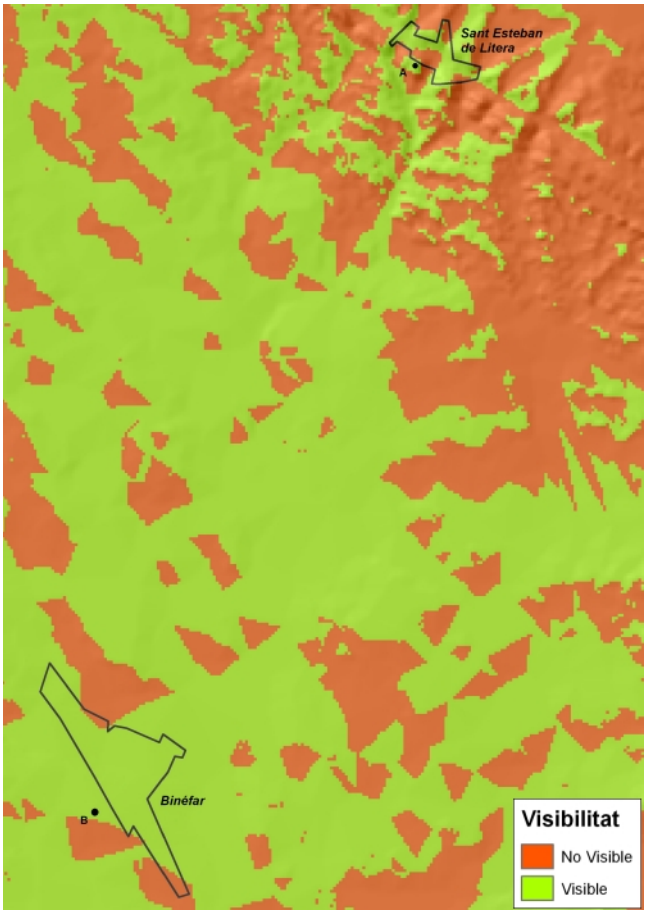


Figura 3.3: Visibilitat San Esteban, antena 15mts., Binéfar, antena 5mts.

3. Antena Binéfar/San Esteban.

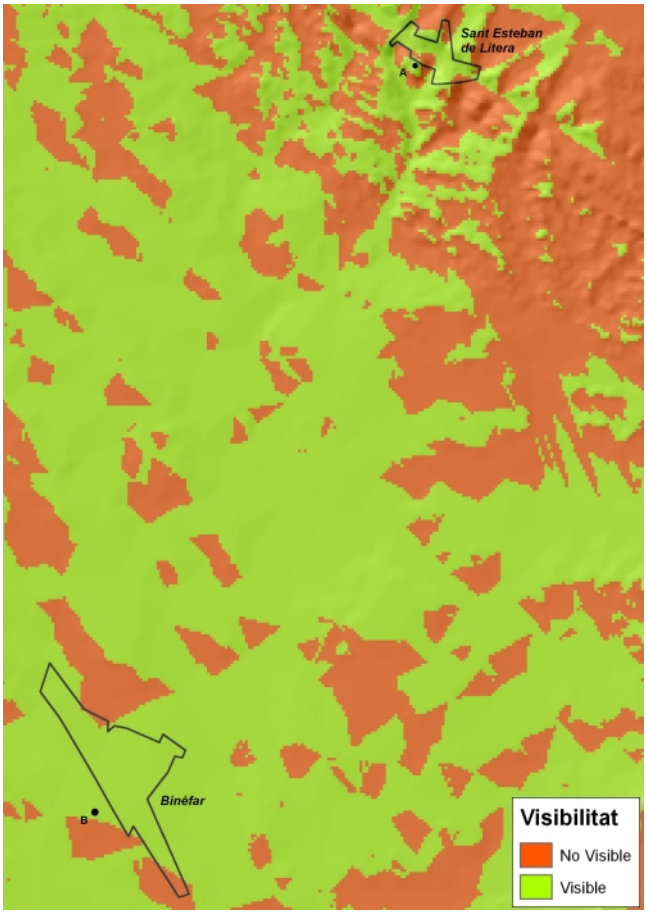


Figura 3.4: Visibilitat San Esteban, antena 20mts., Binéfar, antena 5mts.

4. Antena Binéfar/San Esteban.

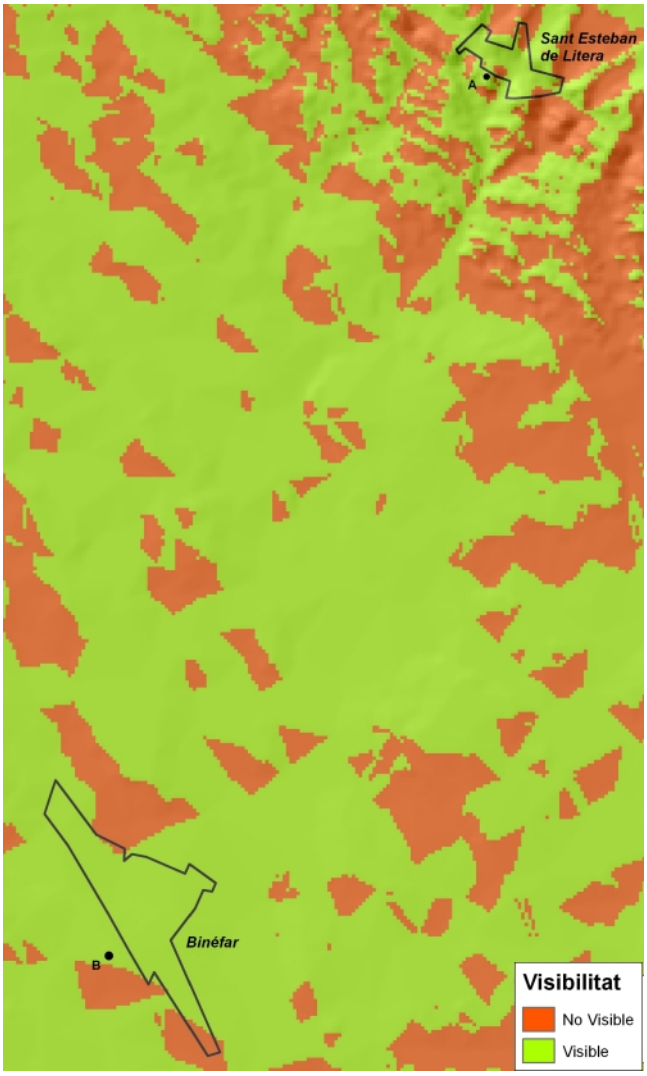


Figura 3.5: Visibilitat San Esteban, antena 25mts., Binéfar, antena 5mts.

Tenint en compte què a la població de San Esteban de Litera disposem d'una torre de comunicacions prèviament instal·lada, i, veient les imatges prèviament

mostrades, s'ha decidit ficar una altura d'antena de 25mts. a San Esteban. Aquesta decisió s'ha basat en els següents criteris:

1. Disposició d'una torre de comunicacions ja instal·lat.
2. Millor visió directa amb una antena de 25 mts.
3. Col·locar un sol AP per a tota la població.

### 3.1.3 Visibilitat San Esteban.

L'estudi de visibilitat a Sant Esteban és molt important. En primer lloc, perquè com ja s'ha comentat abans, estem utilitzant la tecnologia WiFi, a una freqüència de 5GHz, i, aquesta requereix de visibilitat directa entre els punts d'enllaç. I en Segon lloc per determinar quines seran les zones d'ombra, es a dir, les zones del poble on no hi haurà cobertura.

Un cop observada la visibilitat, s'ha decidit utilitzar un única antena per donar cobertura a tota la població, ja que, segons es pot observar en la imatge següent, amb una antena tenim visibilitat a quasi la totalitat de la població.


Figura 3.6: Visibilitat San Esteban, antena 25mts.

## 3.2 Estudi demogràfic.

En aquest apartat, es pretén realitzar un anàlisi del creixement de la població al llarg dels anys, més concretament des de l'any 1900 fins al 2007, i, també,

realitzar un petit estudi de la població que hi ha actualment a San Esteban de Litera. El tipus de població pot ser útil per determinar quanta gent pot necessitar Internet, tenint en compte què els que més l'utilitzen són gent d'entre 10 i 35 anys. Aquest estudi, ens pot ajudar a determinar en quin moment es troba el poble: si és un moment d'expansió o no.

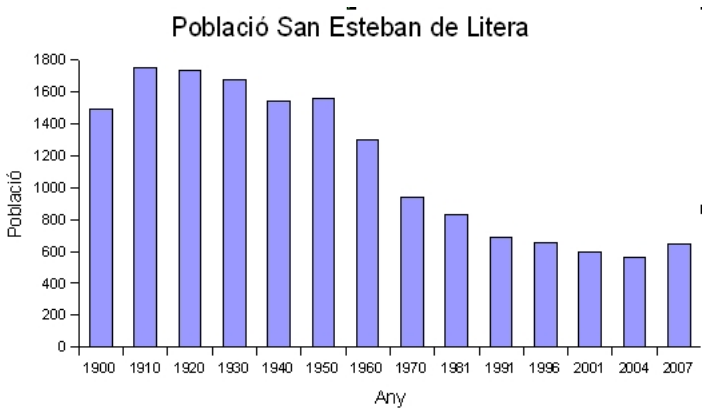


Figura 3.7: Població San Esteban.

| EDATS | Total | Femení | Masculí |
|---|---|---|---|
| TOTAL | 512 | 256 | 256 |
| 0-4 | 3 | 2 | 1 |
| 5-9 | 10 | 5 | 5 |
| 10-14 | 14 | 7 | 7 |
| 15-19 | 10 | 6 | 4 |
| 20-24 | 26 | 10 | 16 |
| 25-29 | 33 | 18 | 15 |
| 30-34 | 35 | 21 | 14 |
| 35-39 | 23 | 13 | 10 |
| 40-44 | 35 | 23 | 12 |
| 45-49 | 23 | 12 | 11 |
| 50-54 | 35 | 16 | 19 |
| 55-59 | 34 | 16 | 18 |
| 60-64 | 42 | 21 | 21 |
| 65-69 | 39 | 20 | 19 |
| 70-74 | 50 | 26 | 24 |
| 75-79 | 38 | 21 | 17 |
| 80-84 | 34 | 13 | 21 |
| 85 i més | 28 | 6 | 22 |

Taula 3.1: Distribució per edats.

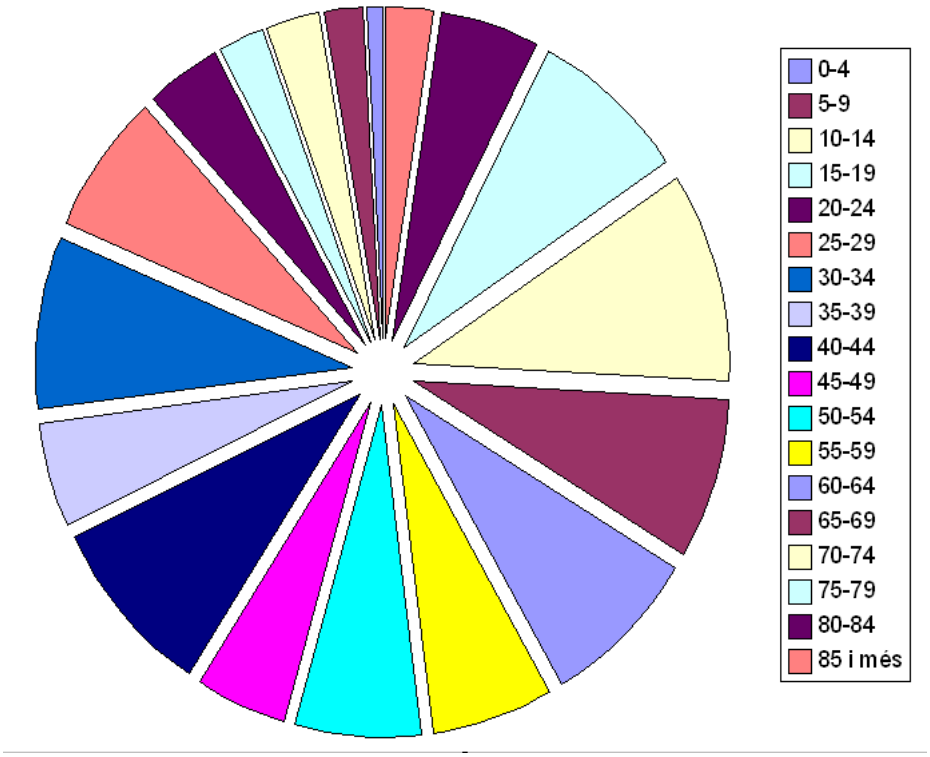


Figura 3.8: Distribució per edats. Femení.

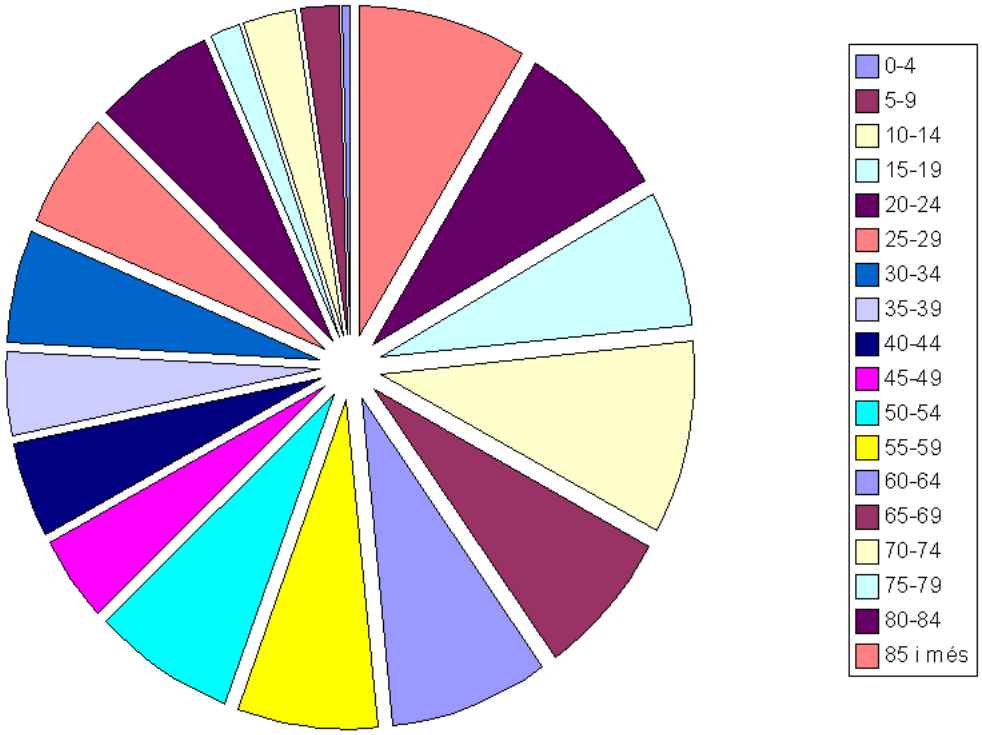


Figura 3.9: Distribució per edats. Masculí.

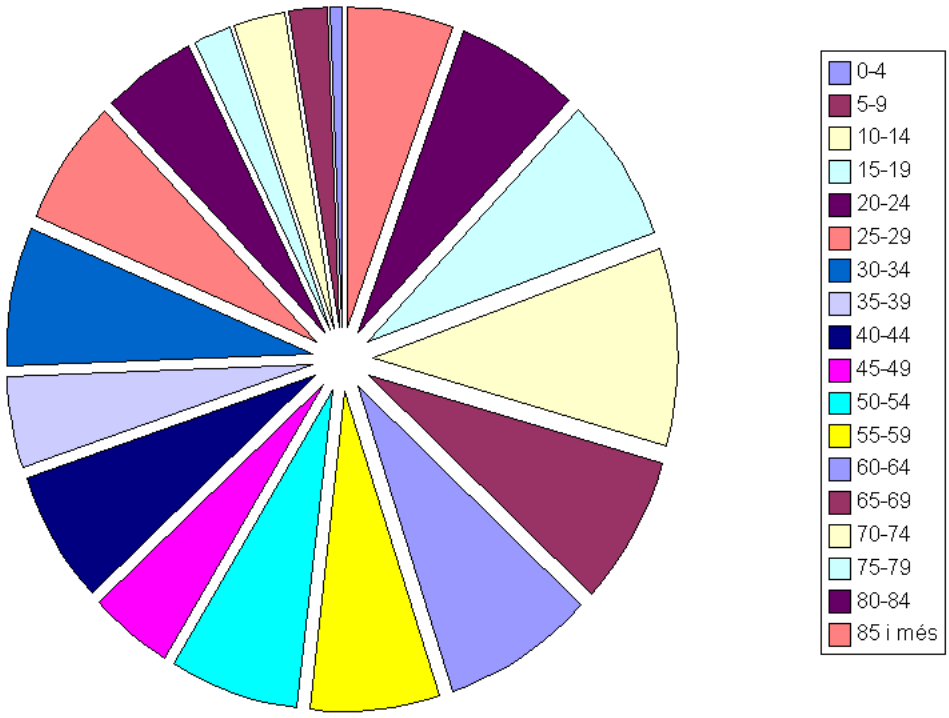


Figura 3.10: Distribució per edats. TOTAL.

# Capítol 4

# Disseny tècnic de la solució.

En aquest capítol s'explicarà com es pot realitzar la instal·lació de la xarxa Wireless d'accés a Internet en el medi rural San Esteban de Litera.
Per tal de donar accés a Internet a San Esteban, s'ha tingut en compte 4 aspectes principals:

1. La connexió ADSL.
2. L'enllaç punt a punt entre Binéfar i San Esteban de Litera.
3. La distribució de la xarxa WiFi dins el poble de San Esteban de Litera.
4. La seguretat de la xarxa.

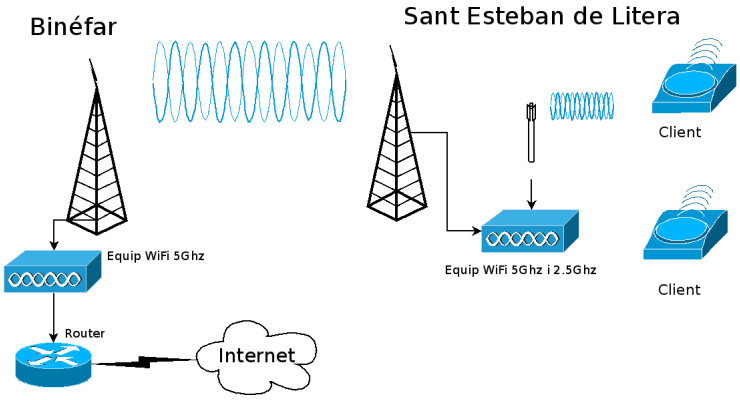


Figura 4.1: Disseny lògic de la xarxa.

## 4.1 Anàlisi de la cobertura Wireless.

Per realitzar l'estudi de cobertura, s'ha fet mitjançant el software lliure Radio Mobile V8.0.5. Amb aquest, hem obtingut els mapes del terreny.

Un cop hem tingut els mapes, el següent ha estat indicar-li on es troben les antenes a comunicar i les característiques de cada antena; Obtingudes les dades, mostra el resultat obtingut de manera gràfica.

Tot seguit, es mostra el resultat obtingut i les característiques de les antenes.

1. Enllaç Punt a punt:

   - Antenes direccionals: 22DBi.
   - Potència dels equips: 500mW.
   - Freqüència: 5GHz

   Cobertura de l'enllaç Binéfar - Sant Esteban de Litera.

   En la figura següent, podem observar com el color negre ens mostra els llocs on arriba la cobertura, emetent des de Binéfar, amb les característiques anteriorment anomenades.

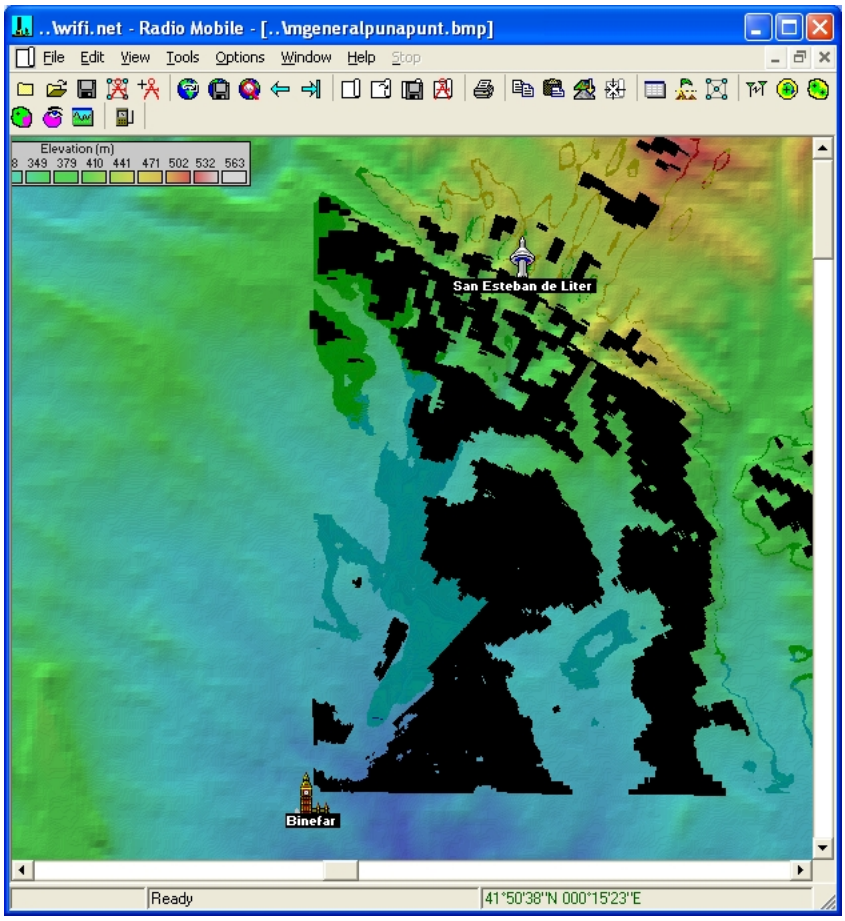


Figura 4.2: Cobertura Binéfar - San Esteban

2. Enllaç punt multipunt:

   – Antena omnidireccional: 10 DBi.

   – Antena Sectorial: 17DBi.

   – Potència de l'equip: 100mW

   – Freqüència: 5GHz

   Cobertura de l'antena situada a San Esteban de Litera.

En el següent dibuix podem observar la cobertura que ens ofereix l'antena i la potència seleccionada, tot i què, no agafa tot el poble, però, sí la gran majoria.

En principi, s'han realitzat tots els càlculs per a un sol AP, situat a Sant Esteban. Si en una futura aplicació es volgués donar cobertura complerta, només s'ha de col·locar un AP dins la cobertura del ja existent, de manera què ampliï la cobertura a la part que falta.

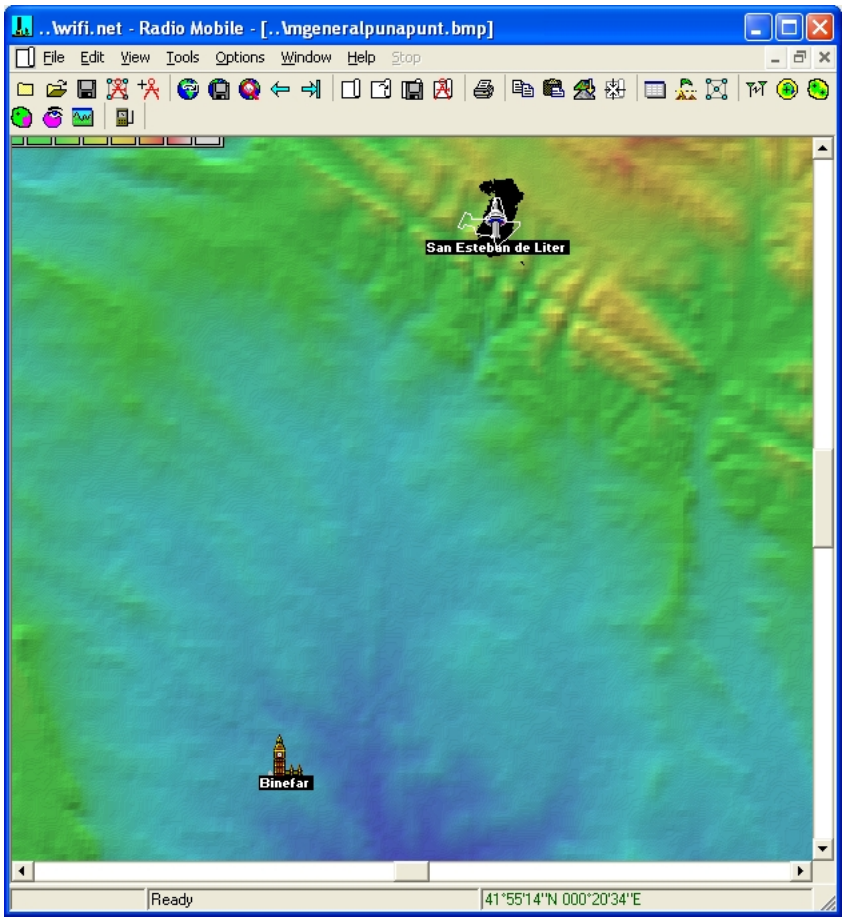


Figura 4.3: Cobertura San Esteban de Litera.

Apunt: No s'ha pogut ampliar més la imatge, degut a que els mapes

cartogràfics de l'Aragó no estan detallats, i els únics que existeixen són militar amb molt baixa qualitat.

## 4.2 Configuració de la xarxa.

En primer lloc, definirem el tipus de topologia que s'utilitzarà per tal de connectar els clients del poble amb el punt d'accés.

L'enllaç entre Sant Esteban i Binéfar, ha de ser un enllaç punt a punt amb antenes directives, en el qual s'haurà de tenir molt en compte la visibilitat entre les dues antenes.

### 4.2.1 Topologia de la xarxa a San Esteban de Litera.

Per realitzar la topologia de la xarxa es tenen dues opcions: infraestructura o Ad-hoc.

La topologia Ad-hoc seria la més indicada per a una connexió puntual entre dos o més equips, però no és fiable per a un nombre elebat d'equips. Per contra, la topologia d'infraestructura ens permet ampliar la xarxa de manera escalar, mitjançant els diferents modes de configuració de cada AP.

Els diferents modes de configuració són: root mode, bridge mode i repeat mode .

La topologia de la xarxa s'aconsella que sigui d'infraestructura.

El mode de configuració del AP de Sant Esteban serà punt - multipunt, ja què, en primer lloc, tenim un enllaç troncal amb Binéfar, el qual es farà amb una antena directiva. I, tenim un enllaç multipunt per a donar cobertura al poble, per tant, necessitarem un altra antena sectorial per donar cobertura.

En resum l'AP de San Esteban ha d'estar dotat de dues antenes: una direccional i una omnidireccional.

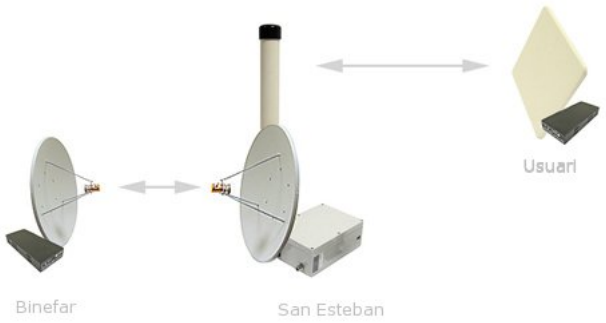


Figura 4.4: Topologia Punt - Multipunt

Característiques de l'equip:

Model: Mikrotik RB/BCO, RouterBOARD 532 with RouterOS L4, caixa externa, dos R52 802.11 a+b+g Wireless miniPCI cards, una antena a 5.7 - 5.8 GHz 10 dBi omnidireccional, una antena a 5.2 - 5.8 GHz 22 dBi direccional, PoE.

### 4.2.2 Connexió ADSL.

Com a ubicació de la connexió ADSL es proposa la gasolinera CRED Binéfar, situada a la Carretera N-240 Núm. 131.


Figura 4.5: Imatge de Binéfar

Tenint en compte les ofertes ADSL, de que podem disposar a Binéfar (1Mbps , 2Mbps, 4Mbps i 8Mbps), tot seguit, es passa a discutir la més adient per al Projecte.

Després de visualitzar les possibles ofertes d'ADSL a les que es té accés en la població de Binéfar, s'ha escollit una connexió ADSL de 8 Mbps.

Per afirmar si la connexió contractada és suficient o no, és realitzen uns càlculs basant-se en una serie de aproximacions.

Si tenim en compte què San Esteban de Litera és una població de 650 habitants, i, contem una mitja de 3 persones per habitatge i amb una connexió Wireless per casascun d'ells, obtenim 650 / 3 = 217 connexions. Amb aquesta dada reflexionem un segons sobre l'ús que es fa de les línies ADSL.

Tal i com passa amb els mòbils, l'ús de la línia no és sempre al 100%, per tant, ens aprofitem del coeficient d'alternança per garantir un servei acceptable en el 80% dels casos.

Basant-nos en els punt anteriors s'han fet les següents aproximacions:

1. El 60 % de la població requereix una connexió a Internet.

2. L'accés a Internet contractat és de 8Mbits/seg.

Amb les aproximacions anteriors s'obtenen els següents càlculs:

1. $650 \bullet 60 / 100 = 390$ Habitants (dividits per 3, resulten 130 connexions).
2. $8000 Kbits/seg / 130 connexions = 61,5$ Kbits/seg / connexió

S'ha de tenir present que les descàrregues per Internet es comptabilitzen en Bytes/seg, i, no en bits/seg com fan els operadors d'accés a Internet, per tant, en una hora de màxima connexió, cada usuari descarregaria a una velocitat teòrica de 61.5 Kbits/seg * (1 Byte / 8 bits) = 7.68 KBytes/seg.

Un cop tenim aquesta dada, es planteja una qüestió:

És suficient aquest ample de banda?

Doncs, depenent de l'ús què es doni a Internet, també, s'ha de tenir en compte que aquesta descàrrega, només es donarà en hores punta. Si el que es vol és Internet per navegar i realitzar descàrregues puntuals, llavors, és acceptable; en canvi, si es vol més ample de banda, caldria pensar en altres solucions com: Internet per satèl·lit, que és molt més car, o contractar més d'una línia ADSL i realitzar un balanceig de càrrega entre les diferents línies.

En cas que la connexió a Internet sigui insuficient, una de les solucions que es proposa és contractar varies línies ADSL i col·locar un switch amb balanceig de càrrega. Si es té més d'una línia d'accés a Internet, amb aquest swtich, aconseguim que les dues línies estiguin ocupades per igual.

### 4.2.3 Enllaç punt a punt, Binéfar i San Esteban de Litera.


Figura 4.6: Ubicació de Binéfar i San Esteban

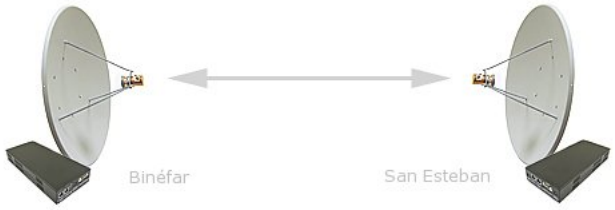


Figura 4.7: Enllaç punt a punt

En l'enllaç punt a punt l'únic que s'ha de tenir en compte és el què s'observa en el dibuix anterior: Dues antenes direccionals, amb un AP cadascuna.

Les dues antenes han d'estar bén direccionades i amb línia de visió directa.

La configuració que ha d'haver-hi en els dos AP's és lleugerament diferent: mentre que a Binéfar tindrem un AP configurat en mode Bridge, ja què, l'únic

que fa és repetir la senyal que li arriba del router; i, en l'altre extrem hi ha un AP configurat en mode AP-Bridge, el qual rep la senyal i la reparteix dins el poble mitjançant una altra antena omnidireccional, com es pot comprovar en l'apartat 4.2.1.

Característiques de l'equip:

Model: Mikrotik RB/BCO amb RouterBOARD 532 with RouterOS L4, caixa externa, dos R52 802.11 a+b+g Wireless miniPCI cards, una antena a 5.2 - 5.8 GHz 22 dBi direccional i PoE.

### 4.2.4 Distribució de la xarxa WiFi a San Esteban de Litera.

La distribució de la xarxa dins el poble es farà mitjançant un punt d'accés situat a la torre de comunicacions de San Esteban de Litera, el qual rebrà la senyal provinent de Binéfar i la repartirà per tot el poble.

Els paràmetres de configuració de la xarxa interna del poble seran els següents:

1. El rang d'IP's a utilitzar seran 192.168.0.0/24.
2. La IP 192.168.0.1/24 es reservarà al AP, el qual, ens direccionarà tota la xarxa del poble per a què vagi dirigida cap a l'AP de Binéfar.
3. Els sistemes de seguretat i totes les proteccions s'aplicaran des de l'estació situada a San Esteban de Litera.

## 4.3 Instal·lació de la xarxa Wireless.

### 4.3.1 Instal·lació dels punts d'accés.

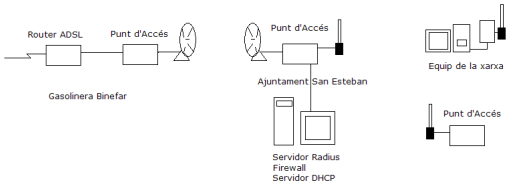


Figura 4.8: Disseny lógic de la xarxa.

La instal·lació dels punt d'accés serà a l'exterior i, depenent del tipus de punt d'accés, enllaç troncal o enllaç de distribució, haurà de tenir unes característiques o unes altres. L'enllaç troncal serà la connexió què uneix Binéfar i San Esteban, per al qual es requereix:

1. Punt d'accés situat a la benzinera de Binéfar:

   Per tal de realitzar la connexió amb el poble de San Esteban i, tenint en compte la distància que hi ha entre els dos pobles, uns 5km aproximadament, s'utilitzarà una antena de tipus paràbola petita. Al ser una antena directiva, el guany que tindrem serà elevat que és el què ens interessa.

   Per realitzar aquesta connexió utilitzarem un guany aproximat de 22DBi's treballant a una freqüència de 5GHz, també hem de tenir en compte que l'equip utilitza la tecnologia PoE per alimentar-se. Per tal d'interconnectar l'antena i el punt d'accés s'utilitzarà un Pigtail N-UFL i es connectarà el punt d'accés amb el router mitjançant un cable Ethernet.

Figura 4.9: Pigtail amb connector N a UFL.

En aquesta part ens apareixen dos conceptes nous: Pigtail i Poe, que tot seguit es passen a comentar:

(a) Poe ( Power Over Ethernet ): La situació dels punt d'enllaç acostumen a ser a l'exterior i, moltes vegades, a altures en les quals ens resulta complicat pujar l'alimentació, ja què, les torres podrien estar situades en llocs poc accessibles. Aquesta tecnologia ens permet

aprofitar dos cables del cable ethernet per tal de transportar corrent al punt d'accés, el qual serà alimentat sense la necessitat de pujar un altre cable per a l'alimentació.

(b) Pigtail: Tal i com es pot comprovar en la fotografia el Pigtail, no és res més que el cable que interconnecta l'antena amb la targeta WiFi, o el punt d'accés. Depenent del tipus de fabricant utilitzat per al punt d'accés, el connector UFL variarà o no; en canvi, el connector de tipus N, habitualment, sempre serà el mateix.

Per tal de garantir la connexió, pel que fa a fallades de la corrent, s'-ha decidit col·locar un SAI (*Sistema d'Alimentació Ininterrompuda*), que estabilitzarà la tensió i subministrarà corrent durant curts terminis de temps.

2. Punt d'accés situat a l'antena de telecomunicacions de San Esteban de Litera.

   En aquest punt d'accés s'utilitzarà la mateixa antena que en el punt anterior i, a més a més, afegirem una antena de tipus panell, la qual, es troba dins la família d'antenes sectorials. Aquesta família ràdia el senyal, aproximadament, uns 180º, i l'antena es troba entre la directiva, que es centra molt en un punt augmentant molt el guany; la omnidireccional reparteix en totes direccions per igual, amb un guany menor.

   En aquest cas, utilitzem una sectorial, amb un guany aproximat de 10 DBi's, perquè l'antena es troba en un extrem del poble, per tant, només ha de radiar en una direcció més amplia que la direccional, però amb més guany que la omnidireccional.

   Pel que fa al punt d'accés, tindrà les mateixes característiques que el de Binéfar, excepte que, haurà de contenir dues antenes en lloc d'una, ja què, en aquest punt, a part de realitzar l'enllaç troncal, s'haurà de donar cobertura al poble. Pel que fa al Pigtail, en aquest cas, en necessitarem dos en comptes d'un.

   Un dels problemes que es podríen trobar en la implantació és què, la gent que es troba més allunyada del AP, no tingui cobertura. Una possible solució, seria instal·lar un AP amb una antena omnidireccional en un lloc estratègic del poble, i, configurar-la en mode WDS, per a què, es comuniqui amb l'AP principal i accepti connexions dels usuaris Wireless.

En aquest punt, també s'instal·larà un SAI per la mateixa raó.

### 4.3.2 Instal·lació estació client.

Cada client que es vulgui connectar a la xarxa Wireless, haurà d'adquirir una estació subscriptora, o estació client, la qual consisteix en el següent:

1. Antena Sectorial amb un guany de 17 DBi's, si s'obtingués més guany, es consideraria una antena direccional i les distàncies no són tant grans com per necessitar una antena direccional. Amb menys guany el que s'obtindria és l'efecte contrari: una antena omnidireccional i, en aquest cas, no ens interessa. Per tant, l'opció sectorial és la més adient. Per tal d'encarar l'antena, s'utilitza un medidor de camp.

2. Client Wireless, serà l'encarregat d'emetre les trames ethernet a la xarxa Wireless, i, rebre les trames Wireless i passar-les a la xarxa ethernet de l'edifici on es troba.

3. Injector de corrent PoE: és el que s'encarrega d'aprofitar dos cables per passar corrent.

   En la següent imatge podem observar la connexió de l'injector de corrent. El connector de l'esquerra és el que es connecta al client Wireless i el connector de la dreta es connecta a l'equip de xarxa o ordinador.

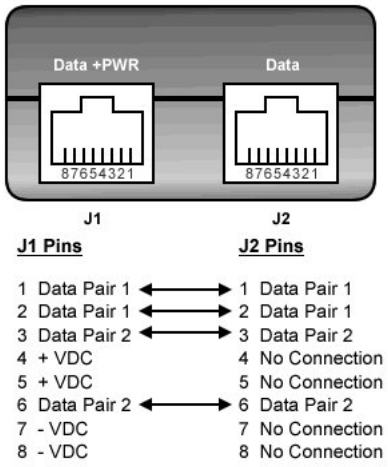


Figura 4.10: Esquema Injector PoE.


Figura 4.11: Injector PoE.

## 4.4 Aspectes de seguretat.

Un dels principals cavalls de batalla de les xarxes inalàmbriques, en vers les xarxes cablejades, és el control d'accés al medi pròpiament dit; un medi que, en el cas de les xarxes cablejades, serà el cable de coure o la fibra òptica, cosa què minimitza les intrusions a tota persona que tingui accés a un punt de xarxa.

Per contra, si tenim en compte que les xarxes inalàmbriques utilitzen com a medi físic l'aire, ens adonarem que un usuari, per connectar-se, no necessita res més que un ordinador amb una tarja inalàmbrica i situar-se en el radi de cobertura.

Si es té en compte aquesta primera aproximació a la realitat, pot ser que ens alarmem i arribem a la mala conclusió de què les xarxes inalàmbriques no son segures.

Si es parteix de la base que res es pot afirmar al 100%, es pot dir que les xarxes inalàmbriques, en l'actualitat, tenen un nivell de seguretat elevat. I, es pot afirmar que una xarxa Wireless ben configurada és tant segura ò, fins i tot, més que una xarxa cablejada.

Un dels principals avantatges en seguretat que tenen les xarxes cablejades en vers les xarxes inalàmbriques bén configurades, és la necessitat d'un punt de xarxa per connectar-se a la mateixa. Però, un cop superat aquest obstacle, l'intrús té via lliure dins la xarxa.

A favor de les xarxes inalàmbriques, a part de requerir un usuari i contrasenya per connectar-se, tota la informació que viatja a través de la xarxa, viatja xifrada, per tant, si un equip es sitúa en el radi de cobertura de la nostra xarxa WiFi, per molt que escolti el nostre trànsit, si no te accés a les claus de xifratge i desxifratge, mai podrà saber quina és la informació que s'envia.

### 4.4.1 Seguretat amb el protocol 802.11a.

El protocol de comunicacions escollit per realitzar tota la implementació és el 802.11a; protocol que utilitza les freqüències lliures de 5Ghz, tal i com, s'ha comentat en el capítol 2.

El protocol de seguretat a utilitzar s'aconsella que sigui el 802.11i, que utilitza encriptació WPA, autenticació 802.1x amb TKIP, AES, i servidor RADIUS. Per tal d'assegurar que és podrà treballar amb el protocol 802.11i, s'ha de tenir en compte aquesta especificació a l'hora de comprar els equips, ja què, degut al protocol WPA2, l'equip de xarxa ha de tenir uns requisits mínims de memòria

i procés.

### 4.4.2 Servidor RADIUS i portal captiu.

El servidor RADIUS és un element molt important de seguretat en l'esquema de xarxa que és proposa.

En primer lloc, s'ha de tenir en compte què, si es vol donar un servei d'accés a Internet, resulta evident que s'ha de realitzar un control d'usuaris, que ens ajudarà a realitzar el servidor RADIUS i el portal captiu.

El servidor RADIUS no és més que una base de dades on s'emmagatzema una sèrie d'usuaris als què, més endavant, es donarà accés.

L'aplicació que acompanya al servidor RADIUS, el portal captiu, no és més que una pàgina WEB implementada en el servidor, on es demana validar l'usuari abans de connectar-se a la Wirless.

Una instal·lació que s'haurà de realitzar en tres punts clarament diferenciats: la instal·lació del servidor RADIUS en la part del servidor, configuració en la part del punt d'accés i configuració en la part del client.

Un cop decidida la instal·lació d'un servidor RADIUS, es presenten diverses opcions: en primer lloc, es podria pensar en instal·lar el servidor RADIUS en un Appliance, és a dir, mitjançant un hardware dedicat; en segon lloc, es pot unificar el firewall, VPN, RADIUS, etc., és a dir, tot el control d'accés des de l'exterior a la nostra xarxa i viceversa, per mitjà d'un Appliance; i, en tercer lloc, configurar un PC o AP com a servidor RADIUS.

La primera opció, seria per a infraestructures molt grans, ja què, tenir un hardware exclusivament per al control dels usuaris que accedeixen a la WiFi, és molt costós, tant a nivell de diners com de manteniment. Es creu que no és la millor solució per aquest cas en concret.

La segona opció seria bona si el control que és volgués fer dels usuaris, fós molt exhaustiu, com seria el cas d'una empresa, és a dir, es necessita d'un plus de característiques, a més d'un firewall i servidor RADIUS, que tampoc és el cas.

Així doncs, la tercera opció és perfila com la més adequada per al Projecte i l'únic que s'ha de decidir és si la implementació del servidor RADIUS serà en l'AP o en un servidor.

En aquest cas, i per tal de no sobrecarregar el AP, s'ha decidit instal·lar el servidor RADIUS en un servidor. A més a més, i per tal de que els usuaris s'identifiquin per accedir a la xarxa WiFi, es realitzara l'instal·lació d'un portal

captiu. Per tal d'aprofitar al màxim el servidor, s'han configurat els següents serveis:

1. Firewall: Filtra els paquets de la xarxa.
2. Proxy: Realitza una caché de les pàgines visitades.

### 4.4.3 Firewall i antivirus.

Tenint en compte què l'ús de la xarxa serà popular i donarà accés a Internet, no es configurarà cap regla restrictiva al Firewall, ni es realitzarà la configuració d'un antivirus centralitzat, ja què, no es pretèn generar un entorn restringit, si no, un entorn obert en el que l'usuari serà l'únic responsable dels seus actes. El que sí s'aconsella als usuaris és, utilitzar un antivirus i alguna protecció del tipus Firewall, per tal de tenir un mínim de seguretat.

### 4.4.4 NAT (*Network address translation*) i Servidors.

La funció NAT ens permet sortir a Internet a través d'una única IP pública, és a dir, el router que proporciona accés a Internet realitza un NAT entre les IP's privades i la IP pública, convertint la IP privada d'un equip de la xarxa Wireless a la IP pública, que utilitzaran tots els usuaris per navegar per Internet.

Aquesta funció s'ha d'implementar per dues raons molt simples: primer, perquè està prohibit sortir a Internet amb IP's privades i, segon, perquè, avui dia, comprar una direcció IP és molt difícil, així com, comprar-ne una per cada usuari de la xarxa Wireless.

En un primer moment, no es contempla configurar cap servidor què doni cap tipus de servei a l'exterior, per tant, no s'aplica cap redirecció.

## 4.5 Configuració del servidor.

Per realitzar la instal·lació física del servidor, es disposa de dues opcions: com a primera opció, instal·lar el servidor en el mateix segment de xarxa que el punt d'accés i instal·lar-lo a San Esteban. En aquest cas, s'han de configurar tots els equips client, per a què realitzin les peticions web al servidor proxy, i, no es podran aplicar les regles firewall sense redireccionar el tràfic des del router ADSL, cosa que alentiria més el tràfic; i, com a segona opció, col·locar el servidor com a pont entre la xarxa Wi-Fi i Internet, que s'aconsegueix amb dues tarjes

de xarxa: una connectada al router ADSL i l'altra connectada al punt d'accés, i, així, tot el tràfic passa obligatòriament pel servidor i aquest aplica les regles pertinents, sense necessitat de configurar cap client.

Per tal d'agilitzar la configuració dels equips client, evitar possibles problemes i perquè es creu que el tràfic generat no saturar el servidor, s'ha escollit la segona opció: instal·lar el servidor com a pont, amb les característiques que s'expliquen a continuació:

La instal·lació del servidor s'ha realitzat amb un S.O. Linux, més concretament, la distribució Kubuntu 7.06. S'ha decidit utilitzar Linux, degut a què es troba sota llicències gratuïtes Open Source.

Els serveis que s'instal·laran i es configuraran al servidor són els següents:

1. Freeradius, Servidor RADIUS, per realitzar el control d'accés.
2. MYSQL, Servidor de Base de Dades, per emmagatzemar la informació dels usuaris.
3. Apache2, Servidor Web, per oferir pàgines web.
4. Apache-SSL, Servidor HTTPS, per oferir connexions segures.
5. Chillispot, Portal Captiu, per realitzar l'accés a través d'una pàgina web.
6. SQUID, Servidor Proxy, per millorar les connexions web.
7. IPTABLES, Firewall, per redireccionar tots els serveis anteriors.

### 4.5.1 Instal·lació i configuració d'un servidor RADIUS.

La Instal·lació i configuració del servidor RADIUS s'ha dividit en els següents punts:

1. Instal·lació i configuració del RADIUS.
2. Configuració de L'Accés Point.
3. Configuració del client Linux per a WPA.

#### 4.5.1.1 Instal·lació i configuració del RADIUS.

El Freeradius és el paquet triat per a realitzar les funcions de servidor RADIUS. S'ha escollit aquest perquè s'integra molt bé amb la distribució de Linux escollida.

En primer lloc, es descarrega el paquet i s'instal·la. Per instal·lar-lo s'obre una consola i s'executa la següent comanda.

*ubuntu:~$ apt-get install freeradius*

Important, per realitzar instal·lacions s'ha de tenir privilegis de root, en cas contrari, s'ha d'anteposar la comanda sudo i, tot seguit, posar la contrasenya d'usuari.

Un cop es té el freeradius instal·lat, es passa a configurar. Els fitxers que s'han de modificar són els següents:

1. En aquest fitxer s'introduirà la xarxa a que es donarà accés.

   /etc/freeradius/clients.conf.

   *#*

   *# clients.conf - client configuration directives*

   *#*

   *#########################################*

   *#########################################*

   *#*

   *# Definition of a RADIUS client (usually a NAS).*

   *#*

   *# The information given here over rides anything given in the*

   *# 'clients' file, or in the 'naslist' file. The configuration here*

   *# contains all of the information from those two files, and allows*

   *# for more configuration items.*

   *#*

   *# The "shortname" is be used for logging. The "nastype", "login" and*

   *# "password" fields are mainly used for checkrad and are optional.*

   *client 192.168.1.0/24 {*

   *secret = pamipipa*

*shortname = private-network-1*

*}*

Tal i com podem observar, es dóna accés a la xarxa 192.168.0.0/24 i la clau compartida que s'ha d'utilitzar per comunicar el freeradius amb els punts d'accés, pamipipa.

2. En aquest fitxer s'introdueix la configuració pròpia del servidor RADIUS.

   /etc/freeradius/radiusd.conf

   *accounting {*

   *#detail*

   *unix*

   *radutmp*

   *sql*

   *}*

3. /etc/freeradius/sql.conf

   *# Connect info*

   *server = "localhost"*

   *login = "freeradius"*

   *password = "radius"*

   *# Database table configuration*

   *radius_db = "radius"*

   En aquest fitxer es configura l'usuari i la contrasenya d'accés a la base de dades.

4. Un cop realitzada la configuració dels fitxers es posa en marxa el servei:

   *ubuntu:/etc/init.d$ ./freeradius start*

#### 4.5.1.2 Configuració de l'Acces Point.

Per tal de dur a terme la configuració de l'Acces Point s'ha de disposar de la següent informació:

- La direcció IP del servidor RADIUS.

- El port del Servidor RADIUS, generalment el 1812.
- La clau compartida.

Com a direcció IP del servidor RADIUS, en aquest cas, s'ha utilitzat la 192.168.0.2. El port del servidor RADIUS és l'estàndard, 1812, i, la clau compartida, serà una clau escollida a l'atzar, per tal d'evitar possibles atacs de força bruta o de diccionari.

Aquesta clau compartida és la que utilitzaran els equips, per tal de, tenir dret a realitzar peticions al servidor RADIUS i, així, poder-se autentificar dins la xarxa WiFi.

#### 4.5.1.3 Configuració del client Linux per WPA.

En primer lloc, i abans de començar la configuració del client, s'han de tenir clars els requisits del client:

1. Targeta Wireless compatible amb WPA.
2. Driver per Linux de la targeta amb suport WPA.

Si es reueixen tots aquests requisits, no es tindrà cap problema en validar-se al portal captiu que sortirà automàticament a l'intentar connectar-se a Internet.

### 4.5.2 Instal·lació i configuració d'un servidor de base de dades.

En aquest cas, el servidor de base de dades escollit ha estat mysql. La decisió s'ha prés en base a tres criteris: és de lliure distribució, és un dels més utilitzats i la seva utilització és molt senzilla.

1. Bé, en primer lloc, s'instal·la els servidor mysql.

   *ubuntu:~$ apt-get install mysql*

2. Degut a què el freeradius necessita una base de dades amb una estructura pre-establerta, es crea la següent base de dades.

   *ubuntu:~$ mysql -uroot* (accedim com a usuari administrador)

   *mysql> CREATE DATABASE RADIUS;*

   *mysql> GRANT ALL PRIVILEGES ON radius.* to 'freeradius'@'localhost' IDENTIFIED BY 'radius';*

*mysql> FLUSH PRIVILEGES;*

Amb aquestes comandes s'ha creat una base de dades 'radius' i se li han assignat privilegis a l'usuari 'freeradius'.

3. Ara s'importarà un fitxer que porta incorporat el freeradius, per tal de crear totes les taules necessàries.

   *mysql> exit*

   *ubuntu:~$ cat /usr/share/doc/freeradius/examples/mysql.sql | mysql -D radius -u freeradius -p radius*

   *ubutnu:~$ mysql -Dradius -ufreeradius -pradius*

   *mysql> INSERT INTO radcheck (UserName, Attribute, Value) VALUES ('jordi', 'Password', '123');*

   Amb l'última comanda, s'ha donat d'alta l'usuari 'jordi' amb contrasenya '123'. Aquesta manera de donar d'alta els usuaris és una mica rústica; el més convenient seria crear una pàgina web per tal d'administrar les altes i baixes (aquesta seria una possible millora de cara al futur).

### 4.5.3 Instal·lació i configuració del servidor web apache2.

El servidor web triat ha estat apache2, perquè és un dels servidors més utilitzat pel que fa a serveis web. També, s'ha tingut en compte, que disposa de llicència lliure Open Source.

1. El primer pas a realitzar serà instal·lar el servidor web.

   *ubuntu:~$ apt-get install apache2*

2. Tot seguit, es crea un fitxer 'index.html' amb la següent informació:

   *<a href="http://192.168.0.2:3990/prelogin">Click here to login</a>*

3. Copiem el fitxer 'index.html' a la carpeta /var/www/:

   *ubuntu:~$ cp index.html /var/www/index.html*

4. Tot seguit, es descomprimeix el fitxer cgi que mostra la pantalla de login:

   *ubuntu:~$ cp /usr/share/doc/chillispot-1.0/hotspotlogin.cgi.gz /var/www/cgi-bin*

   *ubuntu:~$ gunzip /var/www/cgi-bin/hotspotlogin.cgi.gz*

   *ubuntu:~$ chmod 755 /var/www/hotspotlogin.cgi*

5. I, per acabar, es modifica el valor de la variable '$uamsecret' del fitxer 'hotspotlogin.cgi' pel valor 'pamipipa'

   *$uamsecret = pamipipa*

6. Per tal que els cgi-scripts funcionin correctament s'ha de modificar el fitxer /etc/apache2/apache2.conf

   *# AddHandler allows you to map certain file extensions to "handlers":*

   *# actions unrelated to filetype. These can be either built into the server*

   *# or added with the Action directive (see below)*

   *#*

   *# To use CGI scripts outside of ScriptAliased directories:*

   *# (You will also need to add "ExecCGI" to the "Options" directive.)*

   *#*

   *AddHandler cgi-script .cgi*

   *#*

   *# Filters allow you to process content before it is sent to the client.*

   *#*

   *# To parse .shtml files for server-side includes (SSI):*

   *# (You will also need to add "Includes" to the "Options" directive.)*

   *#*

   *Options FollowSymLinks +ExecCGI*

### 4.5.4 Instal·lació i configuració d'un servidor segur, apache-ssl.

Les sigles SSL volen dir en anglès, Secure Socket Layer. S'ha utilitzat aquest servidor per a realitzar comunicacions segures, entre el client que es vol autenticar i el servidor radius. D'aquesta manera, els password i usuaris introduïts viatjaran per la xarxa xifrats.

1. Es descarrega i s'instal·la el paquet.

   *ubuntu:~$ apt-get install apache-ssl*

   Tot seguit, anirà preguntant una sèrie de coses, com el lloc de residència, el correu electrònic, etc. Un cop finalitzades les preguntes, crearà un

certificat que es pot veure en el fitxer /etc/apache-ssl/apache.pem. En aquest fitxer el que s'observa no és res més què una clau privada RSA.

El certificat s'utilitza de la següent manera: el servidor xifra el document amb la seva clau privada. Això limita el desxifratge del document, única i exclusivament, als que tinguin la clau pública; una clau pública què es troba publicada pel mateix servidor. Tot això, permet, a qualsevol client, determinar, mitjançant la clau pública d'aquesta entitat, què aquesta pàgina l'envia l'entitat que s'estava esperant i, per tant, és confiable.

Per damunt dels certificats digitals, hi ha un altre nivell, que són les Entitats Certificadores, les quals s'encarreguen d'emetre certificats i de dir que, aquests certificats, són realment de qui diuen ser. Algunes de les entitats certificadors són: CA (*Certification Authority*), CATCert ( Agència Catalana de Certificació), CESCAT (*Centre de Supercomputació de Catalunya*) que és l'entitat certificadora d'universitats de Catalunya, VeriSign, Inc., entre d'altres.

### 4.5.5 Instal·lació i configuració del portal captiu Chillispot

La principal raó d'haver escollit aquest paquet és, primerament, perquè disposa d'una llicència lliure Open Source, en segon lloc, perquè no disposa de grans opcions, cosa que simplifica el seu funcionament i, en tercer lloc, es troba disponible als repositoris de la distribució triada.

1. Com tots els paquets anteriors es començarà instal·lant el paquet:

   *ubuntu:~$ apt-get install chillispot*

2. Per configurar el portal captiu Chillispot, només s'ha de modificar un únic fitxer, /etc/chilli.conf

   *##########################*

   *#*

   *# Sample ChilliSpot configuration file*

   *#*

   *##########################*

   *# TAG: radiusserver1*

   *# IP address of radius server 1*

```
# For most installations you need to modify this tag.
radiusserver1 localhost
# TAG: radiusserver2
# IP address of radius server 2
# If you have only one radius server you should set radiusserver2 to the
# same value as radiusserver1.
# For most installations you need to modify this tag.
radiusserver2 localhost
# TAG: radiusauthport
# Radius authentication port
# The UDP port number to use for radius authentication requests.
# The same port number is used for both radiusserver1 and radiusserver2.
# Normally you do not need to uncomment this tag.
radiusauthport 1812
# TAG: radiussecret
# Radius shared secret for both servers
# For all installations you should modify this tag.
radiussecret pamipipa
# DHCP Parameters
# TAG: dhcpif
# Ethernet interface to listen to.
# This is the network interface which is connected to the access points.
# In a typical configuration this tag should be set to eth1.
dhcpif eth0
# Universal access method (UAM) parameters
# TAG: uamserver
# URL of web server handling authentication.
uamserver https://localhost/hotspotlogin.cgi
# TAG: uamhomepage
```

*# URL of welcome homepage.*

*# Unauthenticated users will be redirected to this URL. If not specified*

*# users will be redirected to the uamserver instead.*

*# Normally you do not need to uncomment this tag.*

*uamhomepage welcome.html*

*# TAG: uamsecret*

*# Shared between chilli and authentication web server*

*uamsecret pamipipa*

### 4.5.6 Instal·lació i configuració del servei proxy SQUID.

S'ha decidit instal·lar un proxy, per tal de millorar el servei de navegació a través de pàgines web. Els principis fonamentals d'un servidor proxy són els següents:

1. Un client realitza una petició d'una pàgina web al servidor proxy.
2. El servidor proxy comprova si aquesta pàgina ja ha estat sol·licitada.
   (a) En cas afirmatiu, li mostra el contingut de la pàgina que té emmagatzemada.
   (b) En cas negatiu, sol·licita la pàgina web, li mostra al client i l'emmagatzema al seu sistema d'arxius.
3. El servidor proxy s'encarrega de mantenir actualitzades les web que manté en cache.

Per configurar el servidor proxy, tot seguit, s'explica les modificacions que s'han realitzat als fitxers de configuració del servidor:

1. Per instal·lar el servei, com tots els anteriors:
   *apt-get install squid*
2. Configuració del fitxer /etc/squid/squid.conf
   *# Squid normally listens to port 3128*
   *http_port 192.168.1.2:3128*
   *# TAG: cache*
   *# A list of ACL elements which, if matched, cause the request to*

*# not be satisfied from the cache and the reply to not be cached.*

*# In other words, use this to force certain objects to never be cached.*

*#*

*# You must use the word 'DENY' to indicate the ACL names which should*

*# NOT be cached.*

*#*

*# Default is to allow all to be cached*

*#We recommend you to use the following two lines.*

*acl QUERY urlpath_regex cgi-bin \?*

*cache deny QUERY*

*# TAG: cache_mem (bytes)*

*# NOTE: THIS PARAMETER DOES NOT SPECIFY THE MAXIMUM PROCESS SIZE.*

*# IT ONLY PLACES A LIMIT ON HOW MUCH ADDITIONAL MEMORY SQUID WILL*

*# USE AS A MEMORY CACHE OF OBJECTS. SQUID USES MEMORY FOR OTHER*

*# THINGS AS WELL. SEE THE SQUID FAQ SECTION 8 FOR DETAILS.*

*#*

*# 'cache_mem' specifies the ideal amount of memory to be used*

*# for:*

*# * In-Transit objects*

*# * Hot Objects*

*# * Negative-Cached objects*

*#*

*# Data for these objects are stored in 4 KB blocks. This*

*# parameter specifies the ideal upper limit on the total size of*

*# 4 KB blocks allocated. In-Transit objects take the highest*

*# priority.*

```
#
# In-transit objects have priority over the others. When
# additional space is needed for incoming data, negative-cached
# and hot objects will be released. In other words, the
# negative-cached and hot objects will fill up any unused space
# not needed for in-transit objects.
#
# If circumstances require, this limit will be exceeded.
# Specifically, if your incoming request rate requires more than
# 'cache_mem' of memory to hold in-transit objects, Squid will
# exceed this limit to satisfy the new requests. When the load
# decreases, blocks will be freed until the high-water mark is
# reached. Thereafter, blocks will be used to store hot
# objects.
#
#Default:
cache_mem 8 MB
# LOGFILE PATHNAMES AND CACHE DIRECTORIES
# ------------------------------------------
# TAG: cache_dir
# Usage:
#
# cache_dir Type Directory-Name Fs-specific-data [options]
#Default:
cache_dir ufs /var/spool/squid 100 16 256
# ACCESS CONTROLS
# ------------------------------------------
# TAG: acl
# Defining an Access List
```

*# acl aclname acltype string1 ...*

*# acl aclname acltype "file" ...*

*# when using "file", the file should contain one item per line*

*acl INTERNAL src 192.168.1.0/24*

*# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS*

*http_access allow INTERNAL*

*# TAG: visible_hostname*

*# If you want to present a special hostname in error messages, etc,*

*# define this. Otherwise, the return value of gethostname()*

*# will be used. If you have multiple caches in a cluster and*

*# get errors about IP-forwarding you must set them to have individual*

*# names with this setting.*

*#*

*#Default:*

*visible_hostname localhost*

### 4.5.7 Instal·lació i configuració del servei firewall IPTABLES.

IPTABLES és un servei que bé integrat en el KERNEL, nucli del S.O., de LINUX. I, ens permet filtrar les comunicacions entrants i sortints del servidor, mitjançant regles.

Degut a què IPTABLES ja es troba integrat dins el mateix S.O., no s'haurà de descarregar cap paquet addicional. Gràcies a la seva integració en el KERNEL de LINUX IPTABLES facilita molt la seva configuració.

Per configurar aquest servei, s'ha de realitzar un script amb totes les comandes per introduïr les regles que es creguin convenients.

1. Elavoració del script de configuració:

   La configuració serà permisiva, per defecte.

   El signe # ens indica comentari, excepte la primera línia.

   *#!/bin/sh*

```
#
#
# Utilitzem $EXTIF (eth0) per a la interface esterna (Internet) i
# $INTIF (eth1) per a la interface interna (access points).
#
#
# SUMMARY
# * Tote les connexions originades pel Chilli seran permeses.
# * Només SSH sera permess a la interface externa.
# * No es permet res d'entrada a la interface interna.
# * La sortida es pemet si be de la interface externa, però no es permet si be de la interface interna.
# * NAT esta habilitat a la interface externa.
IPTABLES="/sbin/iptables"
EXTIF="eth0"
INTIF="eth1"
INT_NET="192.168.1.2"
# Primer s'eliminen totes les regles existent al firewall.
$IPTABLES -P INPUT DROP
$IPTABLES -P FORWARD ACCEPT
$IPTABLES -P OUTPUT ACCEPT
#Permet les connexión related iestablished en totes les interfaces d'entrada
$IPTABLES -A INPUT -m state –state RELATED,ESTABLISHED -j ACCEPT
#Permet releated, established i ssh a la $EXTIF. La resta no, però informa.
$IPTABLES -A INPUT -i $EXTIF -p tcp -m tcp –dport 22 –syn -j ACCEPT
#Permet related i established si be de $INTIF. Elimina la resta i no genera informe.
```

*# Redireccionem el tràfic tcp port 80 cap al port del servei proxy.*

*$IPTABLES -t nat A PREROUTING -i $INTIF -s $INT_NET -p tcp –dport 80 -j REDIRECT –to-port 3128*

*#Permet el tràfic http i https en totes les interfaces (input).*

*$IPTABLES -A INPUT -p tcp -m tcp –dport 80 –syn -j ACCEPT*

*$IPTABLES -A INPUT -p tcp -m tcp –dport 443 –syn -j ACCEPT*

*#Permet el tràfic tcp port 3990 en totes les interfaces (input).*

*$IPTABLES -A INPUT -p tcp -m tcp –dport 3990 –syn -j ACCEPT*

*#Permet tot el tràfic en la interfaces de loopback.*

*$IPTABLES -A INPUT -i lo -j ACCEPT*

*# Elimina tot el trafic que be de $INTIF (forward)*

*$IPTABLES -A FORWARD -i $INTIF -j DROP*

*$IPTABLES -A FORWARD -o $INTIF -j DROP*

*#Habilita NAT a la sortida del dispositiu.*

*#S'ha decidit no utilitzar NAT ja que el router ADSL ja realitza el NAT pertinent per sortir a Internet.*

*#$IPTABLES -t nat -A POSTROUTING -o $EXTIF -j MASQUERADE*

2. Es carrega el Script a l'arrancar i es fan les següents modificacions :

   – Editar /etc/network/options
   *ip_forward=yes*
   – Es reinicia la xarxa:
   */etc/init.d/networking restart*

## 4.6 La solidesa del sistema.

Per comprovar la solidesa del sistema es proposa dividir les proves en tres nivells diferenciats: cobertura Wireless, velocitat de descàrrega de la línia ADSL i seguretat.

1. Cobertura Wireless: Per determinar la cobertura Wireless a la població de San Esteban de Litera, s'ha realitzat un estudi de visibilitat i un de cobertura, per tal de determinar el nombre de punts d'accés a instal·lar

en la població. L'estudi de visibilitat es pot observar en l'apartat 3.1 i l'estudi de cobertura Wireless en l'apartat 4.1.

2. Velocitat de descàrrega ADSL: Per tal de determinar si la velocitat de descàrrega dels usuaris finals és la correcta, s'aconsella als usuaris que facin un test de velocitat, mitjançant la pàgina WEB http:\\www.adslayuda.com/test-de-velocidad/.

3. Seguretat: Actualment es considera el protocol 802.1x com un sistema segur, gràcies al protocols d'encriptació i el control que realitza el servidor RADIUS, explicats en el segon capítol. Per tant, es considera l'accés a la xarxa WiFi, segur. Per altra banda, també s'ha de tenir en compte un altre tipus de seguretat, com és l'accés des d'Internet a la xarxa WiFi, per a fins mal intencionats. En aquest últim cas, s'ha de conscienciar als usuaris que utilitzin correctament els antivirus, firewalls i demés, per tal de minimitzar aquesta possibilitat.

# Capítol 5

# Pressupost.

En aquest capítol del Projecte s'ha estimat un sol Pressupost.

Com es podrà observar tot seguit, el Pressupost s'ha dividit en tres parts bén diferenciades: la inversió inicial, el cost per usuari i el cost d'explotació.

La inversió inicial, fa referència al cost que suposaria la implantació inicial del Projecte, estudi inicial, hardware, software, instal·lacions, posta en marxa, configuració d'equips, etc. Aquesta part és la més costosa, ja què, requereix d'un estudi inicial molt extens.

La segona part del Projecte, fa referència al cost que suposa la instal·lació d'un equip d'usuari, degut al model que és realitza aquí, s'ha de tenir en compte què, depenent del número d'usuaris que es decideixin connectar a la xarxa, el cost variarà i el número d'altes de clients, que és realitzi de cop, també modificarà el preu de la instal·lació. Per aquestes raons, s'ha cregut convenient realitzar un Pressupost, tenint en compte el pitjor dels casos, és a dir, que cada cop què es dóna una alta, només es dóna la d'un usuari.

La tercera i última part del Pressupost, s'ha dedicat al cost de l'explotació de la infraestructura; un cost que s'ha de tenir molt present, ja què, un Projecte d'aquestes característiques no només requereix d'una inversió inicial, si no què, a més a més, s'ha de tenir present el cost anual que suposa el manteniment de tota la infraestructura i els serveis contractats a tercers.

## 5.1 Pressupost inversió inicial.

Descripció dels treballs: Costos de la inversió inicial, equipament, estudis previs, implantació i instal·lació de l'equipament i configuració dels mateixos.

– Punt 1. Estudis previs, avantprojecte i projecte:

| Número | Descripció | Quant. | Unit. | Preu (Euros) | Total ( Euros ) |
|---|---|---|---|---|---|
| 1 | | | | | |
| 1.1 | Estudis previs i avantprojecte | 40,00 | H | 45,00 | 1.800,00 |
| 1.2 | Projecte | | | | |
| 1.2.1 | Estudi de cobertura i visibilitat | 2,00 | H | 45,00 | 90,00 |
| 1.2.2 | Configuració equips Wireless | 2,00 | H | 45,00 | 90,00 |
| 1.2.3 | Configuració servidor | 16,00 | H | 45,00 | 720,00 |
| 1.2.4 | Legalització instal·lacions | 1,00 | H | 45,00 | 45,00 |
| 1.2.5 | Desplaçaments Almenar - San Esteban - Almenar (1 dia) | | | | |
| 1.2.5.1 | Treballs | 6,00 | H | 45,00 | 270,00 |
| 1.2.5.2 | Desplaçaments | 1,50 | H | 22,00 | 33,00 |
| 1.2.5.3 | Desplaçaments | 100,00 | KM | 0,30 | 30,00 |
| 1.2.5.4 | Dieta dinar | 1,00 | UD | 12,00 | 12,00 |
| | TOTAL 1.2.5 | | | | 345,00 |
| 1.2.6 | Desplaçaments Almenar - Binéfar . Almenar (1 dia) | | | | |
| 1.2.6.1 | Treballs | 6,00 | H | 45,00 | 270,00 |
| 1.2.6.2 | Desplaçaments | 1,00 | H | 22,00 | 22,00 |
| 1.2.6.3 | Desplaçaments | 80,00 | KM | 0,30 | 24,00 |
| 1.2.6.4 | Dieta dinar | 1,00 | UD | 12,00 | 12,00 |
| | TOTAL 1.2.6 | | | | 328,00 |
| | TOTAL 1.2 | | | | 1.618,00 |
| | TOTAL 1 | | | | 3.418,00 |

Taula 5.1: Pressupost inversió incial, punt 1.

– Punt 2. Instal·lacions elèctriques:

| Número | Descripció | Quant. | Unit. | Preu (Euros) | Total ( Euros ) |
|---|---|---|---|---|---|
| 2 | Instal·lacions elèctriques. Muntatge d'una antena. No inclosa antena. | | | | |
| 2.1 | Muntatge i material. | 2,00 | UD | 540,00 | 1.080,00 |
| | TOTAL 2 | | | | 1.080,00 |

Taula 5.2: Pressupost inversió incial, punt 2.

– Punt 3. Adquisició i posta en marxa:

| Número | Descripció | Quant. | Unit. | Preu (Euros) | Total ( Euros ) |
|---|---|---|---|---|---|
| 3 | Adquisició i posada en marxa dels sistemes | | | | |
| 3.1 | Hardware i software | | | | |
| 3.1.1 | Server Opció 1 | 1,00 | UD | 2.702,70 | 2.702,70 |
| 3.1.2 | Server Opció 2 | | UD | 1.717,20 | |
| 3.1.3 | Monitor | 1,00 | UD | 160,00 | 160,00 |
| 3.1.4 | Smart-UPS 750 VA. | 2,00 | UD | 291,60 | 583,20 |
| 3.1.5 | Material Wi-Fi infraestructura. | 1,00 | UD | | 3.000,00 |
| 3.1.6 | Software Open Source | 1,00 | UD | | 0,00 |
| | TOTAL 3.1 | | | | 6.445,90 |
| 3.2 | Posada en marxa | | | | |
| 3.2.1 | Desplaçaments Almenar-San Esteban-Almenar (1 dia, 2 persones) | | | | |
| 3.2.1.1 | Treballs | 12,00 | H | 45,00 | 540,00 |
| 3.2.1.2 | Desplaçaments | 3,00 | H | 22,00 | 66,00 |
| 3.2.1.3 | Desplaçaments | 100,00 | KM | 0,30 | 30,00 |
| 3.2.1.4 | Dieta dinar | 2,00 | UD | 12,00 | 24,00 |
| | TOTAL 3.2.1 | 3,00 | UD | | 1.980,00 |
| 3.2.2 | Desplaçaments Almenar-Binéfar-Almenar (1 dia, 2 persones) | | | | |
| 3.2.2.1 | Treballs | 12,00 | H | 45,00 | 540,00 |
| 3.2.2.2 | Desplaçaments | 2,00 | H | 22,00 | 44,00 |
| 3.2.2.3 | Desplaçaments | 80,00 | KM | 0,30 | 24,00 |
| 3.2.2.4 | Dieta dinar | 2,00 | UD | 12,00 | 24,00 |
| | TOTAL 3.2.2 | 2,00 | UD | | 1.264,00 |
| | TOTAL3.2 | | | | 3.244,00 |
| | TOTAL 3 | | | | 9.689,90 |

Taula 5.3: Pressupost inversió incial, punt 3.

– Especificació dels servidors:

- Server opció 1: SERVIDOR VISA GEA XEON SERIE-510, CPU Intel Xeon 5110P (1.60GHz. 4Mb), DDRAM2 2Gb (4x512Mb) PC2-

5300/667 FBDIMM, Grabadora DVD Dual +-R/RW (NEGRA), Video Integrat, Doble adapt.xarxa integrat (2 x 1GB), Controladora Serial-ATA (6 canales) integrada.

- Server opció 2: NETFRAME PENTIUM 4 VALUE DDRAM2, Intel Core2Duo E6600 (2.40GHz. 4Mb), Memoria DDRAM2 2Gb PC2-4300/533 ECC, Dvd 16x/48x IDE (NEGRO), Video Integrat, Doble adapt. xarxa integrat (2 x 1GB), Controladora Serial-ATA (4 canales) integrada.

– Punt 4. Quotes d'alta:

| Número | Descripció | Quant. | Unit. | Preu (Euros) | Total ( Euros ) |
|---|---|---|---|---|---|
| 4 | Quotes d'alta per als serveis d'operadors (ADSL, satèl.lit, etc.) | | | | |
| 4.1 | Quota alta ADSL 8MB | 1,00 | UD | 0,00 | 0,00 |
| | TOTAL 4 | | | | 0,00 |

Taula 5.4: Pressupost inversió incial, punt 4.

– Punt 5. Inverció inical total:

| | Preu ( Euros ) |
|---|---|
| Total Net Sene IVA | 14.187,90 |
| IVA | 2.270,064 |
| TOTAL | 16.457,964 |

Taula 5.5: Pressupost, preu total inversió inical.

## 5.2 Pressupost Explotació.

En aquest Pressupost s'ha tingut en compte, només, el cost mensual del servei ADSL. Per al cost de manteniment, s'ha fixat un cost orientatiu, cosa que indica que no cobreix qualsevol avaria del sistema.

| Número | Descripció | Quant. | Unit. | Preu (Euros) | Total ( Euros ) |
|---|---|---|---|---|---|
| 1 | Costos de manteniment dels sistemes | | | | |
| | TOTAL | 8 | H | 45,00 | 360,00 |
| 2 | Costos del serveis d'operadors ( ADSL Telefònica 8Mbps. Quota mensual) | | | | |
| | TOTAL | 1 | UD | 158,40 | 158,40 |
| | Total Net sense IVA | | | | 518,40 |
| | IVA | | | | 82.944 |
| | TOTAL | | | | 601.344 |

Taula 5.6: Pressupost explotació.

## 5.3 Pressupost d'usuari.

Cada usuari que es vulgui connectar a Internet, haurà de realitzar una inversió inicial, segons el aquest Pressupost. Cal recordar, i segons diu la legislació actual, comentada en el capítol 2, què no es pot revendre el servei d'Internet gratuïtament. Per tant, l'explotador final de l'infraestructura haurà de decidir, si cobra aquests diners al client i després li cobra una quota, ò, si simplement lloga els equips als clients, mitjançant una quota mensual.

| Número | Descripció | Quant. | Unit. | Preu (Euros) | Total ( Euros ) |
|---|---|---|---|---|---|
| 1 | Instal·lació elèctrica. Muntatge d'una antena | | | | |
| 1.1 | Muntatge. | 1,00 | UD | 260,00 | 260,00 |
| | TOTAL 1 | | | | 260,00 |
| 2 | Adquisició i posada en marxa d'un equip terminal d'usuari | | | | |
| 2.1 | Alta nou usuari | 1,00 | H | 45,00 | 45,00 |
| 2.2 | Material wi-fi infraestructura | 1,00 | UD | 300,00 | 300,00 |
| | TOTAL 2 | | | | 345,00 |
| | Total Net sense IVA | | | | 605,00 |
| | IVA | | | | 96,80 |
| | TOTAL | | | | 701,80 |

Taula 5.7: Pressupost d'Usuari.

## 5.4 Conclusions.

Observant el Pressupost anterior, deduïm què s'hauria de realitzar una inversió inicial de 16.457,964 Euros pel que fa a la infraestructura, després, també, s'ha de tenir present el cost per a cada usuari nou a la xarxa (701,80 Euros). Un cop realitzada la inversió inicial, el cost de manteniment mensual de les instal·lacions bé determinat pel cost d'explotació de 601,344 Euros.

Tot seguit, es passa a analitzar la viabilitat del sistema per a una empresa privada i per a una de pública, utilitzant els pressupostos referenciats anteriorment i les dades de la població referents al capítol 4.

- Si es suposa un màxim de 130 connexions possibles i es suposa un 25% d'usuaris:

  $130 \bullet 25\% = 33\text{Connexions}$

- Si es té en compte la inversió inicial + els usuaris, surt una inversió inicial de:

  $33 \bullet 701,80 = 23.159,40\text{Euros}$

  $23.159,40 + 16.457,964 = 39.617,364\text{Euros}$

- Si realitzem els comptes de manera què, el total de la inversió inicial s'ha de recuperar mitjançant els cobraments mensuals dels usuaris, tenint en compte el cost d'explotació, i s'ha d'amortitzar en un any. S'observen les quotes mensuals següents:

  $39.617,364 / 33 = 1200,53\text{Euros}$

  $1200,53 / 12 = 100,05\text{Euros/mes} \Longrightarrow \text{Amortització del material en 1 any.}$

  $601,366 / 33 = 18,23\text{Euros/mes}$

  $18,23 + 100 = 118,23\text{Euros/mes}$

  - Per a què l'empresa recuperi la inversió realitzada en un any, la quota a establir és de 118,23 Euros al mes per usuari. Aquesta quota, per al tipus de connexió que s'ofereix, és molt abusiva i, per tant, es desestima. Si realitzem els càlculs per tal d'amortitzar la inversió en 3 anys, surt un quota mensual de:

$1.200.53 / 3 = 400,18$Euros/any

$400,18 / 12 = 33,35$Euros/mes $\Longrightarrow$Amortització del material en 3 anys.

$18,23 + 33,35 = 51,58$Euros/mes

- Aquest quota resulta més acceptable, però, per contra, suposa un gran inconvenient per a l'empresa, ja què, un contracte a tres anys, no és fiable per a l'usuari.

– Tenint en compte els càlculs anteriors, es desaconsella realitzar aquest Projecte per a una empresa privada, a no ser que pugui gaudir d'algun tipus de subvenció garantida per l'Estat.

– Pel que fa a l'Administració Pública, els numeros podrien variar lleugerament. En primer lloc, es parteix de la base de què l'Ajuntament que decideixi donar aquest servei, pot disposar dels diners de la inversió inicial, sense tenir en compte el preu per usuari, mitjançant subvencions o altres tipus d'ajuts.

$33 \bullet 701,80 = 23.159,40$Euros

$23.159,40 / 3 = 7719,80$Euros

$7.719,80 / 12 = 643,32 / 33 = 19,50$Euros/mes $\Longrightarrow$Amortització del material en 3 anys.

$601,366 / 33 = 18,23$Euros/mes

$18,23 + 19,50 = 37,73$Euros/mes

– Observant els càlculs anteriors, es dedueix que cada usuari pagarà 37,73 Euros/mes els tres primer anys. A partir d'aquí, l'equip d'usuari passa a ser propietat de l'usuari i la quota mensual de la resta d'anys puja a:

$601,366 / 33 = 18.23$Euros/mes

– Aquesta quota es pot reduïr si el nombre d'usuaris augmenta, ja què, el pressupost d'explotació no depèn del nombre d'usuaris.

# Capítol 6

# Conclusions.

## 6.1 Actualitat de les xarxes.

Des de Internet fins a les LAN, les xarxes han estat, i són, una gran eina per a compartir tot tipus d'informació; una informació que cada cop més, ha resultat ser imprescindible per a la societat en que vivim.

Les xarxes han patit una gran evolució al llarg del temps, des de les xarxes militars, les quals permetien compartir informació estratègica, precursores de l'Internet actual, fins a les xarxes més actuals, en les què podem trobar arquitectures client - servidor, serveis de VoIP, compartir tot tipus de fitxers, serveis de vídeo sota demanda i molts més serveis que, en l'actualitat, ens ofereixen les xarxes.

Una de les principals limitacions de les xarxes ha estat i és, l'ample de banda. Tothom s'haurà adonat que no es necessita el mateix ample de banda per compartir un arxiu de text què, per compartir un fitxer de vídeo; Ò, no es necessita el mateix ample de banda per compartir un vídeo què, per visualitzarlo on-line; ò, no es necessita el mateix ample de banda per compartir un fitxer què, per compartir un fitxers, i, a la vegada, utilitzar el servei de VoIP.

Els protocols de comunicació i la codificació de la línia, han estat els principals causants de que l'ample de banda hagi augmentat fins a l'actualitat.

A part de l'ample de banda, un altre dels handicaps que tenien les xarxes, era la necessitat d'un cable per connecta-se a la xarxa, cosa que deixa moltes zones geogràfiques, com les zones rurals, sense possibilitat de connexió. Aquesta falta s'ha substituït mitjançant enllaços amb ones radioelèctriques ò, el que és el

mateix, amb connexions inalàmbriques, mitjançant protocols Wireless, WiMAX, Bluetooth, infrarojos, etc.

En l'actualitat, les xarxes Wireless, el seu màxim exponent és la connexió de llocs inaccessibles per al cable, com podria ser: donar accés a Internet a l'àmbit rural; un àmbit què, degut a la reduïda població dels seus nuclis urbans, a les operadores no els resulta rentable cablejar la zona. Per tant, la única solució que ens queda per comunicar-les és: utilitzar l'aire com a medi de transport.

Per tal que la comunicació sigui fiable, s'han tingut que desenvolupar nous estàndards de comunicació, com són Wireless o WiMAX, entre altres.

Una de les principals batalles de les xarxes inalàmbriques és l'àrea de cobertura i, com no, l'ample de banda ofertat; un ample de banda, que amb l'entrada en escena de WiMAX, s'ha vist millorat substancialment, ja què, fins al moment, Wireless només ofereix amples de banda de 54 Mbps; en canvi, WiMAX ho amplia fins a 124 Mbps, a part, també, d'augmentar considerablement la distància de cobertura, que passa de 300 mts. amb Wireless a 40 - 70 km amb WiMAX, sens dubte una notable millora.

Però, no tot són avantatges, ja què, la tecnologia WiMAX encara està en una primera fase de proves i, de moment, els costos d'implantació són molt més elevats que els de la tecnologia Wireless.

Pel que fa a la implantació de xarxes inalàmbriques, podem trobar empreses, com IBERBANDA, que es dediquen a oferir aquest servei mitjançant el protocol WiMAX, amb freqüències de 3.5Ghz.

Un altra companyia que dóna connexió a petits nuclis rurals és AWACATE, que utilitza el protocol Wireless amb freqüències de 5Ghz.

També, podem trobar empreses com el moviment FONT, que ofereixen, a tots els qui disposin d'una connexió ADSL, compartir-la inalàmbricament, perquè tots els usuaris del moviment FONT es puguin connectar en un determinat moment, incloent, també, dins de la oferta, la possibilitat de revendre una part de l'ADSL, per a què altres és puguin connectar.

Per altra banda, també podem trobar xarxes lliures, regides per llicències que faciliten la distribució i l'us de continguts per al domini públic, com pot ser CCL(*Creative Commons License*), per a què es tingui una idea de la llicència. El que ve a dir, a grans trets, és el següent:

1. No se'n pot fer un ús comercial.

2. La distribució, i còpia dels continguts, és lliure, referenciant l'autor i l'origen.

3. Es poden modificar els continguts i fer-ne treballs derivats si el resultat es distribueix de nou sota les mateixes condicions.

Basant-se en aquesta llicència, podem trobar xarxes inalàmbriques creades per ciutadans, que no donen accés a Internet, i, l'únic que pretenen és interconnectar el màxim nombre de màquines possibles i compartir informació entre elles. La idea és la mateixa que Internet però, de moment, està en una fase molt reduïda.

Un dels moviments que promou aquestes idees és guifi.net, la qual, a Catalunya, consta de més de 2500 punts d'accés operatius i més de 1000 projectats.

Així doncs, tal i com podem observar, les opcions que hi ha avui en dia són molt variades; tot depèn de les necessitats que requerim. Si el que es requereix és molt tràfic, s'haurà de mirar una connexió amb molt ample de banda i si el problema que es té és de impossibilitat de connectar-se a Internet, doncs, es tenen opcions privades de connexió inalàmbrica. Per contra, si el que es vol és crear una xarxa alternativa, es pot tenir en compte què ja hi ha Projectes molt interessants en marxa.

## 6.2 Els grans operadors i el món rural.

Fins fa relativament poc, l'accés a Internet s'ha realitzat aprofitant al màxim les qualitats de la RTB (Red Telefónica Básica), amb tecnologies com xDSL, RDSI o ISDN (*Integrated services digital network*), entre altres.

Les velocitats ofertes han variat al llarg de tot aquest temps, des de 56 Kbps fins a 20Mbps.

En tot aquest temps, les centrals telefòniques han requerit alguna que altra adaptació, com és el cas del salt dels 56Kbps al xDSL. Per realitzar aquest salt es necessita d'una certa adaptació per part de les centrals telefòniques, per tant, tots aquells pobles que tinguin telèfon però la centraleta no estigui preparada, no podrà donar el salt a la tecnologia xDSL, i, tot i que estigui preparada, si el cablejat no està en condicions o si la distància de l'usuari final a la central és molt elevada, el servei serà deficient. S'ha de tenir present en aquests casos què, per contracte, les companyies només estan obligades a oferir el 10% de la oferta.

Per intentar solucionar el problema de la baixa velocitat i l'elevat preu de l'accés a Internet, tot i l'aplicació de la liberalització del mercat de les telecomunicacions, els nous operadors estan intentant cablejar amb fibra òptica; una

fibra òptica que en l'actualitat permet unes velocitats a l'usuari final, de 20 Mbps.

Degut a l'esforç que comporta desplegar aquesta infraestructura i als costos que l'acompanyen, a més del 50 % de les llars Catalanes, encara no es pot gaudir d'aquesta tecnologia.

Un altra oferta que ha sorgit a arrel del mal funcionament de la xarxa convencional en zones rurals, i, la negativa de les operadores a donar cobertura xDSL en localitats petites i apartades dels nuclis urbans més poblats, s'han vist afectats pel retrocés tecnològic.

Una de les actuacions, ha estat l'adjudicació de projectes de xarxes inalàmbriques en el món rural per part dels governs de les comunitats autònomes, els quals estan adjudicant els projectes en diferents fases.

En el cas de Catalunya, actualment, està en la fase d'actuar en nuclis urbans que superen els 100 habitants. També, esta previst reduïr aquest requisit en properes fases, per tal d'arribar a tota la població.

Una de les empreses beneficiàries d'aquestes adjudicacions, pel que fa a Catalunya, és IBERBANDA, la qual, està realitzant la cobertura inalàmbrica mitjançant WiMAX amb les freqüències privatitzades de 3,5 Ghz.

# Apèndix A

# Acrònims

**LAN** Local Area Network

**WiMAX** Worldwide Interoperability for Microwave Access

**WiFi** Wireless Fidelity

**IEEE** he Institute of Electrical and Electronics Engineers

**WLAN** Wireless Local Area Network

**NLOS** Non-line-of-sight

**MAC** Medium Acces Control

**WLAN** Wireless Local Area Network

**BSS** Basic Service Set

**AP** Acces Point

**DS** Distribuitio Sistem

**ISO/OSI** International Organization for Standardization/Open Systems Interconnection

**WDS** Wireless Distribution System

**MACA** Medium Access Collision Avoidance

**SMA/CA** Carrier Sense Multiple Access with Collision Detection

**RTS/CTS** RTS/CTS

**WLAN** Wireless Local Area Network

**IAS** Internet Authentication Service

**RADIUS** Remote Authentication Dial In User Service

**WEP** Wired Equivalent Privacy

**WPA** Wi-Fi Protected Access

**TKIP** Temporal Key Integrity Protocol

**MIC** Message Integrity Check

**EAP** Extensible Authentication Protocol

**WLAN** Wireless Local Area Network

**CCMP-AES** Counter Mode with Cipher Block Chaining Message Authentication Code Protocol - Advanced Encryption Standard

**IPSec** Internet Protocol Security

**O.S.** Operating System

**LDMS** LANDesk Management Suite

**LOS** Line Of Sight

**QPSK** Quadrature Phase-Shift Keying

**16QAM** Quadrature Amplitude Modulation

**SLA** Service Level Agreement

**QoS** Quality Of Service

**VoIP** Voice over Internet Protocol

**OFDMA** Accés Múltiple per Divisió Ortogonal de Freqüència

**ADSL** Asymmetric Digital Subscriber Line

**CS** Convergente Sublayer

**CPS** Common Part Sublayer

**AAS** Adaptive Antennas System

**ARQ** Automatic Retransmision Request

**STC** Space Time Coding

**ATM** Advanced Traffic Management

**Tx** Transmissor

**Rx** Receptor

**DES** Data Encryption Standard

**RSA** Rivest Shamir Adleman

**PDU** protocol data unit

**CRC** Cyclic Redundancy Check

**Admón** Administració electrònica

**CNAF** Quadre Nacional d'Atribució de Freqüències

**CEPT** Conférence Européenne des administrations des Postes et des Télécommunications

**ISP** Internet Service Provider

**PSSI** Prestador de Serveis de la Societat de la Informació

**SIG** Sistema d'Informació Geogràfica

**Poe** Power Over Ethernet

**GNU** GNU is Not Unix

**NAT** Network address translation

**CCL** Creative Commons License

**ISDN** Integrated services digital network

**SAI** Sistema d'Alimentació Ininterrompuda

**DNS** Domain Name Server

**IP** Internet Protocol

**CA** Certification Authority

**CESCAT** Centre de Supercomputació de Catalunya

# Bibliografia


[1] Pàgina Web del ministeri, http://www.mityc.es/Telecomunicaciones/Secciones/Espectro/

[2] Institute of Electronic and Electrical Engineers IEEE, http://www.ieee.org, 802.11b-1999.pdf, 802.11a-1999.pdf, 802.11a-1999.pdf

[3] IEEE Project 802.16, http://ieee802.org/16/pubs/80216e.html

[4] IEEE 802.11 Wireless Local Area Networks, http://www.ieee802.org/11/

[5] Whitepaper, "Principalesestándaresinalámbicos", Jalercom S.A. http://jalercom.com/Brochures/brochure_tecnologia-wireless.pdf

[6] Pàgina web del WiMAX Forum, http://www.wimaxforum.org/home/

[7] Pàgina Web de la WiFi Alliance, http://www.wi-fi.org/

[8] Pàgina Web del CMT, http://www.cmt.es

[9] Wikipedia, ca.wikipedia.org, en.wikipedia.org, es.wikipedia.org

[10] William Stallings, "Comunicaciones y Redes de Computadores", 7ª Edició, Editorial Pearson Prentice Hall

[11] Comunitat Wireless lliure, http://www.guifi.net

[12] Comunitat Wireless lliure, http://www.sincables.net

[13] Hardware wireless http://www.mikrotic.com

[14] IBERBANDA, http://www.iberbanda.com

[15] I2CAT, http://www.i2cat.cat

[16] Software Radio Mobile, http://www.cplus.org/rmw/english1.html

[17] Apunts Xarxes I , Capítol 3, Enric Guitart, EPS

[18] IEEE Working group 802. Http://www.ieee802.org

[19] Cuadro Nacional de Atribución de Frecuencias (CNAF), http://www.setsi.mcyt.es/espectro/cnaf.htm.

[20] Moviment FONT, http://www.fon.com/es/info/whatsFon

[21] Comunitat Ubuntu, www.ubuntu-es.org

[22] Buscador http://www.google.com